PC PROFESSIONELL SONDERHEFT

SONDERHEFT SICHERHEIT

PC PROFESSIONELL

EXPERT EDITION

Deutschland: € 7,95 02/04
Österreich: € 8,75 Luxemburg: € 9,30 Schweiz: CHF 15,90

# Der große Security-Guide

# Windows Sicherheit Netzwerk

GRATIS

## Auf der Heft-CD




PC Professionell Security-Kit




GhostSurf 2.0 Express*




AVG AntiVirus 6.0 FE*




Version Backup 2.10




Pest Patrol Express*




Sygate Personal Firewall 5.5 Standard*

H+BEDV DATENTECHNIK GMBH
Antivir Personal Edition 6.23

ZONE LABS
ZoneAlarm 4.5

* kostenlose Online-Registrierung nötig

## Das müssen Sie wissen:

- PC & Daten optimal schützen
- Die besten Sicherheits-Tools
- Überwachung im Büro verhindern
- Datenklau beim Surfen erkennen
- Spam-Mail-Angriffe stoppen

4 199043 507952 02

# Sicherheitsexperte »Administrator«


## IMPRESSUM

**Verlag**
VNU Business Publications Deutschland GmbH
Riesstraße 25, 80992 München
Telefon: (089) 143 12-0, Fax: (089) 14 31 21 00
(ist zugleich Anschrift aller Verantwortlichen)

**Chefredaktion** Christoph Scholze
– verantwortlich für den redaktionellen Teil –
**Chef vom Dienst** Annette Völkel

**Redaktionelle Mitarbeit**
Dr. Andreas Bloom, Bertold Brackemeier, Konstantin Breyer, Daniel Dubsky, Martin Goldmann, Stefan Greiner, Oliver Ibelshäuser, Heiko Mergard, Ralf Nebelo, Dirk Reichelt, Eric Tierling, Bettina Weßelmann, Britta Widmann

**Schlussredaktion** Annette Völkel

**Design & Layout** Karsten Gorissen
**Bildbearbeitung** Karel Hajek

**Anzeigenleitung**
Jörg Mühle (verantwortlich)
**Anzeigendisposition** Sabine Hess -264

**Direktor Vertrieb/Vertriebsmarketing**
Karl-Heinz Berthold
**Vetrieb Handelsauflage**
MZV Moderner Zeitschriften Vertrieb GmbH & Co. KG, Breslauer Straße 5, 85386 Eching
Telefon: (089) 319 06-0, Fax: (089) 319 06-113

**Produktionsleitung** Brigitte Gorissen
**Druck und Bindung** R. Oldenbourg, Heimstetten

**CD-Produktion** Stroemung GmbH



**Urheberrecht**
Alle in diesem Sonderheft erschienenen Beiträge sind urheberrechtlich geschützt. Alle Rechte, auch Übersetzungen, sind vorbehalten. Reproduktionen gleich welcher Art, ob Fotokopie, Mikrofilm oder Erfassung in Datenverarbeitungsanlagen, nur mit schriftlicher Genehmigung des Verlags. Aus der Veröffentlichung kann nicht geschlossen werden, dass die beschriebene Lösung oder verwendete Bezeichnung frei von gewerblichen Schutzrechten ist.

**Haftung**
Für den Fall, dass in diesem Sonderheft unzutreffende Informationen oder in veröffentlichten Programmen oder Schaltungen Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlags oder seiner Mitarbeiter in Betracht. Für unangefordert eingesandte Manuskripte, Datenträger, Produkte und Fotos wird keine Haftung übernommen.

© 2004 VNU Business Publications Deutschland GmbH



**Publisher**
Jörg Mühle
**Geschäftsführer**
Jonathan Ross


Netzwerk-Sicherheit, Server-Angriffe und Datenverluste, das sind die Top-Themen in aktuellen Newslettern. Niemals zuvor waren mehr Viren, Würmer und Trojaner unterwegs, noch nie wurden mehr Spam-Mails verschickt.

Administratoren sollten jedoch in der ganzen Patch- und Service-Pack-Hektik einen wichtigen Punkt nicht außer Acht lassen: Neben der regelmäßigen Aktualisierung der Software ist eine durchgängige Sicherheits-Strategie für das gesamte Netzwerk das A und O. Für jedes Bedrohungsszenario müssen die passenden Gegenmaßnahmen in der Schublade parat liegen. Was passiert, wenn Sie einen Hacker-Angriff bemerken? Dürfen Sie das gefährdete Produktions-Netz einfach vom Rest der Welt trennen oder steht dann sofort Ihr Chef in der Tür und droht, Sie für den entstandenen Schaden aufkommen zu lassen? Trauen Sie sich überhaupt, einen erfolgten Angriff oder die wahre Zahl der Spam-Mails bekannt zu geben oder gar einen Testangriff mit gefährlichsten Viren auf Ihr eigenes Netzwerk zu starten? Wie reagiert Ihr Unternehmen auf Angriffe, die nicht verhindert werden konnten – aktiv mit Benachrichtigung aller Kunden oder wird der Fall einfach totgeschwiegen?



»Eine klare Sicherheitsstrategie ist unumgänglich. Das Einspielen einzelner Patches und Service-Packs hilft nur am Rande.«

Mit dem Einspielen von Updates ist es nicht getan. Sie müssen eine wirksame Sicherheits-Strategie entwickeln, sich mit Ihren Vorgesetzten absprechen und vor allem die Gegenmaßnahmen im Falle eines Angriffs auf das Netzwerk üben, üben und nochmals üben.

Viel Expertenwissen und die richtigen Technologien sind gefragt, will man sich gegen die Gefahren der globalen Datenkommunikation schützen. Die Initiative müssen Sie selbst mitbringen, die neuesten Sicherheits-Techniken zeigen wir Ihnen auf 100 Seiten in diesem Security-Sonderheft.




**Bertold Brackemeier**
**Redakteur Netzwerk**
bertold_brackemeier@vnu.de

PC PROFESSIONELL
EXPERT EDITION




Editorial / Impressum 3
CD-Inhalt 97

## TECHNIK

Angriffsziel PC 7
Chef-Spionage 10
LAN in Gefahr 16
Falsche Fährten 18
Tarnen & Täuschen 22
Malicious XML 26
XP-Verschlüsselung 30
Nie allein im Web 34
Longhorn: Die nächste Stufe 38
Drahtlos unsicher 44
Security-Services 46

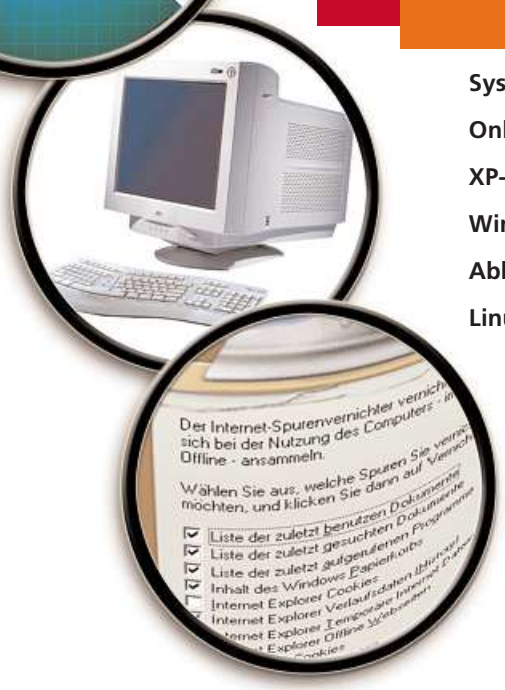


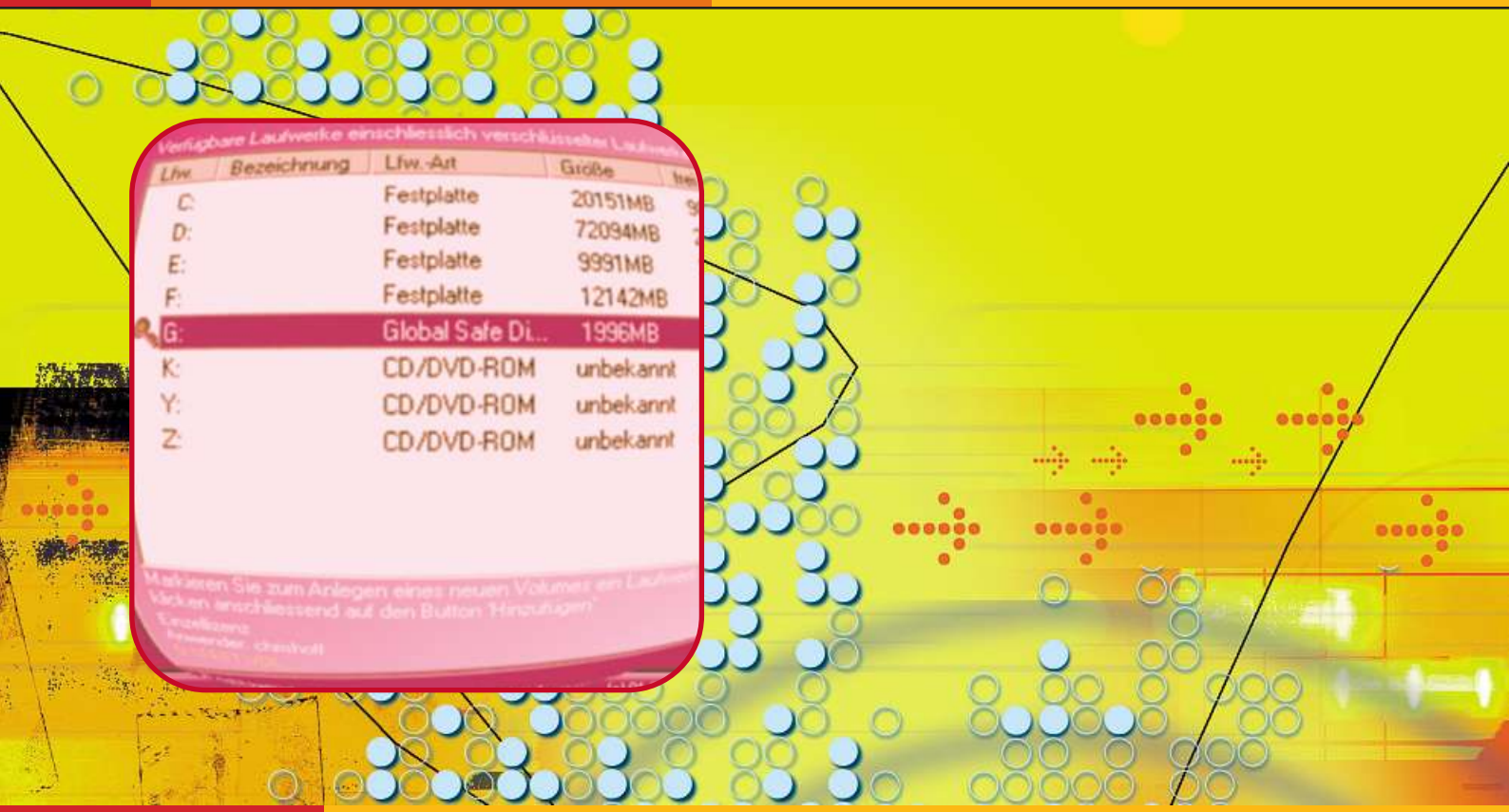

## VERGLEICHSTEST

Client-Virenschutz 50
Kammerjäger 54
Hardware- und Software-Firewalls 58
E-Mail-Spam-Filter 63
Spam-Abwehr 70

## PRAXIS

System-Spitzel 76
Online-Checks 82
XP-Sicherheit 84
Windows-98-Schutz 87
Abhörsicher 90
Linux-Spam-Filter 93






# Technik

Netzwerk-Server und -Clients sowie Privat-PCs sind ständigen Bedrohungen ausgesetzt. Hackerangriffe aus dem Internet, speziell präparierte Webseiten, Viren, Trojaner und sogar Kollegen versuchen sich Zugang zu Ihren Daten zu verschaffen. Lesen Sie, wie die Angreifer dabei vorgehen und wie Sie sich schützen können.

## INHALT

7 **Angriffsziel PC**
10 **Chef-Spionage**
16 **LAN in Gefahr**
18 **Falsche Fährten**
22 **Tarnen & Täuschen**
26 **Malicious XML**
30 **XP-Verschlüsselung**
34 **Nie allein im Web**
38 **Longhorn: Die nächste Stufe**
44 **Drahtlos unsicher**
46 **Security-Services**

# Angriffsziel PC

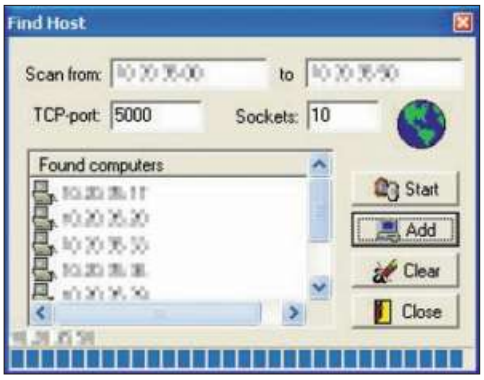
**Um sich vor Datendieben und Hackern aus dem Web zu zu schützen, sollten die gängigen Tricks bekannt sein. So fällt es leichter, Sicherheitslücken zu schließen.** Oliver Ibelshäuser




Das Internet bietet umfangreiche Informationen zu allen denkbaren Themen, kostenlose Software, Filme und verlockende Gewinnspiele. Doch unter der bunten Oberfläche lauern Gefahren. So ist es Angreifern mit den passenden Werkzeugen möglich, einen PC binnen Sekunden auszuspionieren und lahm zu legen. Auf der dunklen Seite des Web agieren Hacker ebenso wie automatische Bots mit Mal- und Spyware. Täglich finden allein in Deutschland zwischen 500 und 1000 gefährliche Hacker-Angriffe auf Firmennetze statt. Die Zahlen der automatisierten Angriffe auf PCs von Privatanwendern liegen um ein Vielfaches darüber. Bei mehr 65 000 Ports bieten sich Angreifern zahlreiche Wege in das System und wieder hinaus. Für Anwender, die viel online sind, sollte das Absichern ihres Systems die oberste Priorität haben. Individuelle Nutzungsgewohnheiten und Rechnerkonfigurationen erfordern individuell angepasste Sicherheitskonzepte. Home-User müssen sich vor allem vor Web-Attacken von außen schützen, Business-User auch gegen Attacken von innen. Denn rund 80 Prozent aller Angriffe auf Unternehmen erfolgen aus dem Intranet oder mittels eines physikalischen Zugriffs. Grundsätzlich gilt jedoch: Anwender können Hackern Zugriffe nur erschweren, hundertprozentig verhindern können sie diese nicht.

## Kostenloser Minimalschutz

Einen ersten Schutz gegen den unbefugten physikalischen Zugang zum PC stellen bereits das abgeschaltete Booten von Diskette, CD-ROM oder USB-Stick, Bios- und Windows-




**▲ Ein Trojaner wie Netbus sucht selbstständig nach IP-Adressen mit einem offenen Port und stellt die Verbindung der Anwendungen her.**

Passwörter sowie das Verschlüsseln wichtiger Daten dar. Software-seitiger Schutz beginnt bei der Installation. Standardroutinen sollten vermieden werden, da diese Pfade und Konfigurationen allen Hackern bekannt sind. Aktuelle Patches und Updates für jede installierte Software vom Betriebssystem bis zum Mediaplayer und Browser schließen viele, wenn auch nicht alle Sicherheitslücken.

Zudem ist es wichtig, die Rechte von Programmen wie etwa Webzugriffe und von Benutzern weitestgehend einzuschränken, denn die meiste Malware nutzt genau diese vorhandenen Benutzerrechte aus. Internet-Sicherheit beginnt damit, Funktionen wie beispielsweise Java, Javascript, Active Scripting und ActiveX auf ein Minimum zu beschränken. Mehr Sicherheit bedeutet dann aber auch weniger Komfort.

## Business perfekt absichern

Kleine Büros wie Arztpraxen, Kanzleien und mittelständische Wirtschaftsunternehmen benötigen ein weitaus höheres Maß an Sicherheit als Privat-PCs. Denn Datenmissbrauch gefährdet dort das gesamte Unternehmen und dessen Kunden. Deshalb sollte jeder PC über einen Diebstahlschutz verfügen, wie ihn etwa Kensington mit dem Desktop-Microsaver anbietet. Auch Floppy-Laufwerke lassen sich mit Schlössern verriegeln. Wichtige Programme wie Patientendatenbanken müssen über ein eigenes Zugangs-Passwort verfügen. Dienstliche E-Mails werden mittels Verschlüsselung und Signatur geschützt.

Netzwerke und Server sollten kleine Unternehmen mit einer klassischen Firewall-Appliance schützen. Virenscanner sind im Netz für alle Clients und den Server einzurichten. Auch ein zusätzlicher Spam-Filter für den Mail-Server ist sinnvoll. Größere Netzwerke benötigen vollständige Content-Security-Systeme wie Mimesweeper. Für das schnelle Reagieren auf Angriffe eignen sich Intrusion-Detection-Systeme (IDS). Zum Einstieg empfiehlt sich das kostenlose Open-Source-IDS Snort *(www.snort.org)*.




**▲ Verschlüsselte Laufwerke können in Global Safe Disk sehr einfach hinzugefügt und auf Mausklick aktiviert werden.**

## Spezialfall Verschlüsselung

Einzelne Dateien und Verzeichnisse lassen sich auf jedem PC mit Programmen wie zum Beispiel Fine-Crypt *(www.finecrypt.net)* und der Freeware Easy Crypto Deluxe 5.5 *(www.handybits.com/easycrypto.htm)* verschlüsseln und nur mit dem entsprechenden Passwort öffnen. Allerdings muss hier der Anwender immer selbst aktiv werden, um etwa die Verschlüsselung zu aktivieren.

Empfehlenswert und sicherer ist das Verschlüsseln gesamter Partitionen oder Festplatten. Die kommerziellen Programme Cyprotect Disk-Encryption *(www.cyprotect.com)*, Global Safe Disk *(www.globalsafedisk.com)*, Drive Crypt *(www.securstar.com)* und Steganos Safe *(www.steganos.de)* bieten dazu entsprechende Funktionen. Alternativ lassen sich auch verschlüsselte Container-Dateien anlegen, die auf unverschlüsselten Festplatten abgelegt werden. Über einen eigenen Laufwerkbuchstaben ist der Zugriff unter Windows wie gewohnt möglich. Selbst der Ausbau der Festplatte führt nicht zum Ziel, die verschlüsselten Daten bleiben unlesbar.

Verschlüsselungsalgorithmen mit 128 oder 256 Bit sind momentan mit realistischem Aufwand nicht zu knacken. Drive Crypt integriert sogar eine Verschlüsselung mit 1344 Bit. Einen guten Mittelweg unter Windows XP Professional stellt das NTFS-Dateisystem mit aktiviertem EFS (Encrypting File System) dar. OIB

# Chef-Spionage

**Der Arbeitsplatz-PC ist ein schlechter Geheimnisträger. Über spezielle Tools liest der Chef jeden Tastendruck mit – sofern sich der Anwender nicht wehrt.**

Oliver Ibelshäuser



Jeder Arbeitnehmer in Deutschland mit einem eigenen PC-Arbeitsplatz könnte vom Chef überwacht werden. So lassen sich mit Hilfe des Netzwerk-Administrators eine Vielzahl relevanter Informationen zusammen tragen. Diese ergeben dann im Idealfall ein lückenloses Profil: Wann hat der Angestellte mit der Arbeit begonnen? Wie lange war er in Pausen? An wen wurden E-Mails verschickt? Welche Dateien hat der Mitarbeiter geöffnet, bearbeitet oder gelöscht? All diese Fragen lassen sich mit Hilfe von gespeicherten Netzwerk-Protokollen beantworten. Illegal ist diese Form der Überwachung nicht, solange die Observierung der Firmensicherheit dient und nicht auf einzelne, willkürlich ausgewählte Personen beschränkt ist.

## Bossing: Mobbing ist Chefsache

Experten sehen derzeit einen Trend zum so genannten Bossing in Deutschland. Zwar sind heimliche Überwachungsmethoden, die das Persönlichkeitsrecht des Opfers verletzen, verboten. Dazu zählen Telefonmitschnitte, das Lesen privater Mails und geheimer Dokumente sowie das Installieren von Spy-Software Rechnern der Mitarbeiter. Wie viele deutsche Arbeitgeber sich aber an das Verbot halten, ist nicht bekannt.

Die USA gehen dieses Thema liberaler an – aus Sicht der Arbeitgeber. Dort ist fast alles erlaubt, was nützlich ist, um unbequeme Arbeitnehmer loszuwerden. Wirtschaftsforscher der amerikanischen Privacy Foundation *(www.privacyfoundation.org)* schätzen, dass in den USA mindestens 30 Millionen PC-Arbeitsplätze überwacht werden. Tools fertigen Screenshots an und informieren den Chef bereits beim Eintippen bestimmter Schlüsselbegriffe. Nachteil für die Opfer: Da die Schnüffelsoftware sehr diskret arbeitet, bleibt die Überwachung zunächst unbemerkt.

## Der gläserne Anwender im LAN

PC-Anwender im Büro sollten sich darüber im Klaren sein, dass es im Netz oder Cyberspace keine Privatsphäre gibt. Zwar verzichten die meisten Administratoren darauf, die zahllosen, täglich anfallenden Protokolldateien auszuwerten, sofern keine besonderen Umstände vorliegen – aus technischer Sicht wäre das aber unproblematisch. Die mögliche Observierung erstreckt sich übrigens nicht nur auf Ordner und Laufwerke, die im Netz freigegeben sind. Je nach LAN-Infrastruktur stehen dem Admin auch lokale Verzeichnisse offen.

## Jede E-Mail ist öffentlich

E-Mails und Briefe haben eine Gemeinsamkeit: Die Post wird in jeder Firma geöffnet und auf die entsprechenden Fächer der Mitarbeiter verteilt. Dort könnte theoretisch jeder die Briefe seiner Kollegen einsehen oder sogar ungelesen wegwerfen. Schon daher käme niemand auf die Idee, sich private Post ins Büro senden zu lassen. Das sollte auch für E-Mails gelten, denn in puncto Datenschutz gelten die

gleichen Spielregeln. Alle Mails, die auf dem Firmen-Account einlaufen oder darüber versendet werden, sind öffentlich, zumindest für die Netzwerk-Mitarbeiter. Es ist zwar nicht vorstellbar, dass ein Systemoperator täglich mehrere tausend E-Mails liest. Über Content-Filter lassen sich aber interessante Nachrichten automatisch herausfischen.

Ein Großteil dieser Überwachung dient allein der Sicherheit und dem reibungslosen Ablauf der Unternehmenskommunikation. In der Regel werden Daten in folgenden Fällen erhoben: zur Netzbelastung, zu Fehlern beim Datentransfer, zur Einhaltung der Sicherheitsrichtlinien, zur Auslastung von Laufwerkskapazitäten sowie zur Software-Nutzung. Primär dienen diese Informationen nicht dazu, Mitarbeiter genau zu überwachen, obwohl dies durchaus möglich wäre.

Letztlich laufen User-abhängige Daten immer an den Knotenpunkten in einem Netzwerk zusammen, beispielsweise am Gateway (Firewall, Virenscanner, Proxy-Server) sowie am Mail- und Fileserver. Wertet der Administrator die Logfiles aus, ist er in der Lage, sämtliche Schritte aller Anwender im Web, im lokalen Netz und teilweise auch auf der lokalen Festplatte mitzuschreiben. Im Normalfall sind die Protokolle nur bei technischen Störungen von Belang. Dementsprechend werden diese Aufzeichnungen nur für wenige Tage gespeichert und dann gelöscht.

## Systemüberwachung der Server

Windows-Server-Systeme stellen unter Zuhilfenahme des Verzeichnisdienstes Active Directory firmeninterne Sicherheitsrichtlinien sicher. So stehen beispielsweise (Netz-)Anwendungen nur bestimmten Anwendern zur Verfügung, das Editieren der Registry ist auf allen administrierten Maschinen verboten oder alle Anmeldeereignisse werden täglich mitgeschrieben. Mit solchen Loggings erfährt der Vorgesetzte nicht nur, wer zuerst kommt und geht, sondern auch, mit welchen Programmen sich der Mitarbeiter beschäftigt. Zudem hat der Administrator via Active Directory die Option, einzelne Windows-Funktionen auf dem lokalen PC zu blocken, um Sabotage zu verhindern.

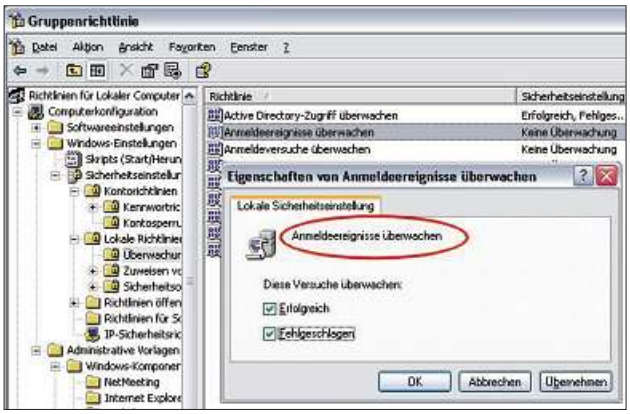
Kontrolle und Verbote sind aber nicht lückenlos, da der Administrator nur solche Anwendungen verbieten kann, die das System von sich aus bereitstellt. Wenn beispielsweise der Befehl *regedit* untersagt ist, lässt sich die Registry dennoch bearbeiten, wenn es dem Anwender gelingt, ein lauffähiges Registry-Programm auf eine Diskette oder einen USB-Stick zu packen und von dort aus zu starten.

## Überwachung in Windows XP

Ein Teil der Überwachungs- und Kontrollfunktionen der aktuellen Windows-Server-Systeme findet sich in abgespeckter Form auch in Windows XP. Somit ist jeder Anwender ansatzweise in der Lage, seinen Rechner zu administrieren, als handle es sich um einen Server. Die angemeldeten Personen müssen sich dann den zugeschriebenen Rollen fügen. Über die Gruppenrichtlinien *(gpedit.msc)* definiert der Systemadministrator, wer was auf dem System darf. Windows stellt dem Benutzer dazu über die Sicherheitsrichtlinien von Haus aus ein Set vordefinierter Policys zur Verfügung, das der Administrator lediglich aktivieren muss. OIB

**Der Administrator hat auch auf Ordner Zugriff, die der User nicht explizit im Netz freigibt. ▼**




**▲ Gruppenrichtlinien überwachen auch in Windows XP erfolgreiche und gescheiterte Anmeldeversuche.**

# Der gläserne Anwender in der Firma

**Im Gegensatz zur administrativen Überwachung ist die personenbezogene Spionage verboten. Viele Chefs registrieren dennoch jeden Tastendruck der Mitarbeiter und werten die Informationen aus.**

Oliver Ibelshäuser

Wie viele deutsche Angestellte mit Hilfe administrativer oder spezieller Tools pausenlos überwacht werden, ist nicht bekannt. Experten schätzen aber, dass jeder zehnte PC-Arbeitsplatz im Visier der Vorgesetzten ist. Das heißt, der Chef ruft heimlich persönliche Daten vom PC des Überwachten ab, ohne den Betroffenen darüber zu informieren.

Die meisten Opfer verfügen nur selten über das entsprechende Know-how und die Möglichkeiten, die Überwachungseinrichtungen auf dem Arbeitsplatz-PC zu entdecken und deren Einsatz nachzuweisen.

## Spionage-Programme

Grundsätzlich lassen sich zwei Klassen von Spionage-Programmen unterscheiden: Netzwerk-Programme protokollieren User-Aktivitäten im Netz, wie etwa Internet-Zugriffe oder den E-Mail-Verkehr. Eine lokale Überwachung findet nicht oder nur ansatzweise statt. Zur zweiten Klasse zählen Spy-Tools, die lokal installiert werden und auf dem PC des Opfers in regelmäßigen Abständen Screenshots anfertigen und nach Belieben alle Tastaturanschläge protokollieren.

Vor allem an den ein- und ausgehenden Mails der Mitarbeiter zeigen viele Chefs Interesse. Anhand der Nachrichten lässt sich exemplarisch feststellen, welcher Mitarbeiter auf der Suche nach einer neuen Anstellung ist, welcher sein Privatvergnügen vor den Pflichten einreiht oder sogar Firmengeheimnisse ausplaudert. Den Denunzianten-Job übernehmen Content-Filterprogramme, die sich direkt im Mailserver einklinken. Der Anwender merkt davon nichts. Diese Tools operieren mit variablen Negativ-Listen und schlagen bei bedenklichen Inhalten Alarm. Dabei kann es sich um einzelne Wörter oder auch unerwünschte Dateiformate der Attachments handeln. Ebenfalls im Visier stehen die Webseitenaufrufe, die Rückschlüsse darüber zulassen, wie stark die Angestellten privaten Interessen nachgehen. Dazu gehört etwa das Lesen von Newseiten, das Steigern bei E-Bay oder das Abrufen von Börseninformationen für das private Aktienportfolio.




▲ **Mail-Content-Filter verhindern das Aussenden unerwünschter Attachments – hier die neue Single »Bad Day« der Popgruppe REM als MP3-File.**

## Mails und Web-Aufrufe im Visier

Mimesweeper von Clearswift *(www.clearswift.de)* ist eines der am weitesten verbreiteten Netzüberwachungs-Tools. Das Programm kümmert sich um Verstöße gegen die von der Firma definierten Regeln innerhalb digitaler Nachrichten und auch beim Surfen. Mimesweeper gibt es in unterschiedlichen Versionen – je nach Überwachungsinteresse und eingesetztem Mailserver. Der Internet-Filter von Mimesweeper for Web ist in der Lage ist, bestimmte URLs zu blocken. Das ist eine offene Kontrolle, da der Anwender die Auswirkungen sofort spürt. Außerdem kontrolliert das Tool Down- und Uploads. Die Server-Anwendung Mailsweeper durchleuchtet alle ein- und ausgehenden Mails nach bestimmten Regeln. Dafür stellt der Administrator eine Liste verdächtiger Schlüsselwörter und Dateianhänge zusammen.

Abgerundet wird die Spy-Palette von Imagemanager. Das ist eine Erweiterung für Mailsweeper, die bei Dateianhängen eine Bilderkontrolle durchführt. Ermittelt das Programm bei Bilddateien mit überwiegend Hauttönen einen Schwellenwert, schrillt der vermeintliche Porno-Alarm.

## E-Mail-Überwachung inklusivie

Orangebox Mail von Cobion *(www.cobion.de)* überprüft auf Wunsch zusätzlich die in E-Mails eingebetteten Hyperlinks, analysiert Bilder auf mögliche pornografische Inhalte und entpackt Archive zur Kontrolle im Bedarfsfall automatisch.

Surfcontrol *(www.surfcontrol.com)* bezeichnet sich selbst als Weltmarktführer von ser-

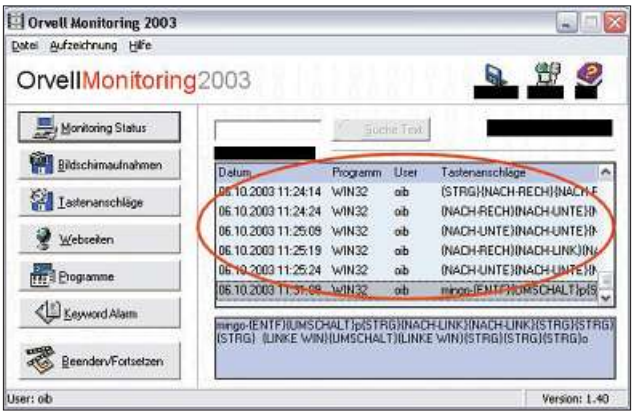
verbasierten Spionage-Tools für Internet und Mail-Client. Das Unternehmen bietet mehrere Versionen der Agenten-Software an, abhängig von der jeweils eingesetzten Plattform für die installierten Mailserver.

Auch Webspy *(www.webspy.com)* hat einen festen Platz unter den leistungsstarken Observierern. Das wichtigste Programmmodul, Sentinel, ist ein leistungsstarkes Monitoring-Tool, das die Surfwege der User überwacht und E-Mails durchleuchtet. Damit Sentinel nichts entgeht, klinkt sich das Tool direkt an der Netzwerk-Karte des überwachten Rechners ein und arbeitet wie ein Sniffer. Damit aber nicht genug: Mit dem Live-Modul lassen sich Angestellte in Echtzeit auskundschaften. Auf Wunsch aktiviert der Vorgesetzte eine Alarmfunktion, die heimlich anspringt, wenn das Opfer gegen eine Regel der Negativlisten verstößt. Es gibt zahllose weitere Programme, die eine Anwenderüberwachung mit ähnlicher Funktionalität vornehmen und ein- und ausgehende E-Mails anhand von Negativlisten in »gut« und »böse« unterteilen. Dagegen wehren kann sich der Anwender auf zweierlei Weise. Zum einen ist das systematische Ausspionieren auch privater Mails verboten und damit ein Fall für den Betriebsrat. Zum anderen kann der Anwender private Attachments so tarnen oder schützen, dass diese den Inhalt garantiert nicht freigeben.

## Lokal installierte Spy-Tools

Subversiver als Netzwerk-Tools arbeiten lokale Überwachungsprogramme. 007 Starr, Orvell, Winston und andere Spy-Tools sind nicht auf funktionierende Netzwerk-Verbindungen angewiesen, um jede Tastatureingabe mitzuverfolgen. Das Protokoll wird nämlich lokal angelegt. Natürlich können sich Netzwerk-Verantwortliche die Daten automatisch schicken lassen, etwa wenn das Opfer bestimmte verbotene Begriffe eingibt oder pikante Webseiten besucht. Diese firmeninterne Indexliste lässt sich beliebig erweitern. Auch Boss Everywhere, ISpy Now, E-Blaster, Winston, Investigator oder Win-Protokoll arbeiten nach einem ähnlichen Prinzip.

Der Betroffene hat kaum eine Chance, die Big-Brother-Methoden zu bemerken. Die Spy-Tasks laufen sehr speicher- und prozessor-schonend ab, hinterlassen nur wenige Spuren auf der lokalen Festplatte und in den Systemeinstellungen und schicken im Bedarfsfall nur kleine Pakete über die Leitungen. Deswegen registriert das Opfer keine Geschwindigkeitseinbußen.




◀ **Das Programm Orvell schreibt detailliert jeden Tastendruck mit, um Passwörter abzufangen oder E-Mails mitzulesen.**

## Profi-Spione und Keylogger

Grundsätzlich lassen sich zwei Typen von lokal agierenden Spy-Tools unterscheiden: Suite-ähnliche Komplettpakete, die eine ganze Reihe unterschiedlicher Spionageaufgaben wahrnehmen, sowie Keylogger, deren einzige Aufgabe darin besteht, Tastatureingaben mitzuschneiden.

Zum funktionalen Repertoire der Suiten (etwa Orvell, Starr, Winston) gehören Bildschirmfotos in regelmäßigen Abständen, das Protokollieren von aufgerufenen Internet-Seiten, gestarteten Programmen und Dateien, das Aufzeichnen von Tastaturanschlägen, das Verstecken der eigenen Tasks und das Anlegen von Logfiles. Einige Programme erstellen zudem komplette Videofilme der Desktop-Aktivitäten.

Orvell *(www.orvell.de)* von Protectcom lässt sich einfach konfigurieren, arbeitet in einem ausgeklügelten Stealth-Modus, verbraucht nur minimale Ressourcen und übernimmt fast jeden erdenklichen Spionage-Auftrag auf dem PC des Mitarbeiters. Real Spy gehört dazu, ein Tool, das sich auch in Hacker-Kreisen sehr großer Beliebtheit erfreut.

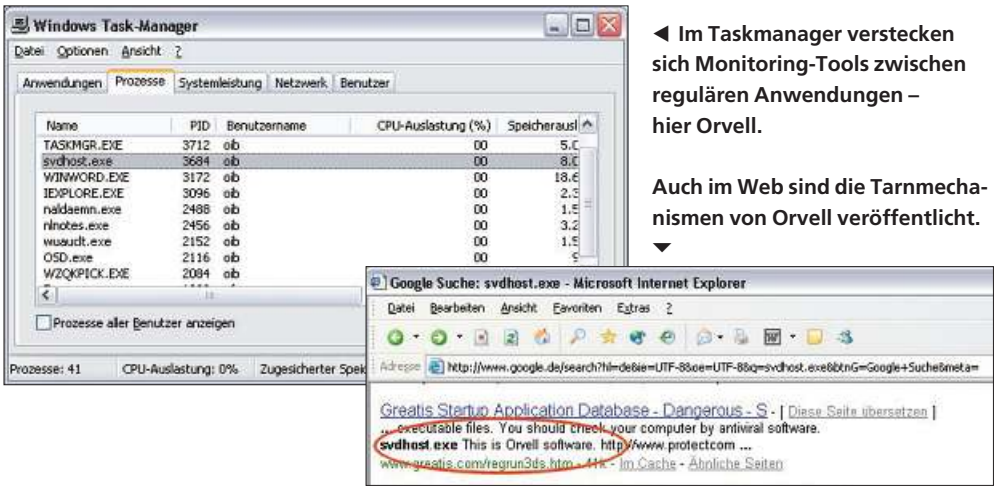
Keylogger haben es auf Passwörter, Kreditkarteninformationen oder sonstige geheime Eingaben abgesehen. Die meisten dieser Snooper kommen ohne grafisches Interface aus und arbeiten befehlszeilenorientiert. Die Verwandtschaft der Keylogger zu Trojanern ist sehr groß. Mittlerweile enthalten auch fast alle aktuellen Viren wie etwa Sobig.F eine entsprechende Backdoor-Komponente, die per Internet-Zugriff in der Lage ist, den Keylogger zu laden. Zu den beliebtesten Keyloggern zählen Chat Nanny, Key-Interceptor, Key-Log und Key Key Professional von Mikko Technology, das unter dem fadenscheinigen Vorwand, »künftig keine eingetippten Informationen mehr zu verlieren« als Backup-Lösung angepriesen wird. OIB

# Spyware und Keylogger demaskieren

**Lokal installierte und aktive Spionageprogramme lassen sich mit Windows-Bordmitteln, kostenlosen Helfern und Profi-Tools schnell entlarven und rückstandslos aus dem System verbannen.**

Oliver Ibelshäuser

Das Hauptproblem der Anwender bei der Fahndung nach Malware sind nicht die mehr oder weniger ausgefeilten Spy-Programme, sondern die Konfigurations-Rechte auf dem eigenen PC. Arbeitet der Anwender in einem voll administrierten Domänen-Netzwerk, bestehen unter Umständen nicht einmal ausreichend Rechte, um einen erforderlichen Microsoft-Patch aus dem Internet zu laden. Eine Identifizierung der digitalen Wachhunde ist allerdings nur möglich, wenn sich Autostart-Ordner, Taskmanager, Registry und Systemverzeichnisse bearbeiten lassen.




**◀ Im Taskmanager verstecken sich Monitoring-Tools zwischen regulären Anwendungen – hier Orvell.**

**Auch im Web sind die Tarnmechanismen von Orvell veröffentlicht. ▼**

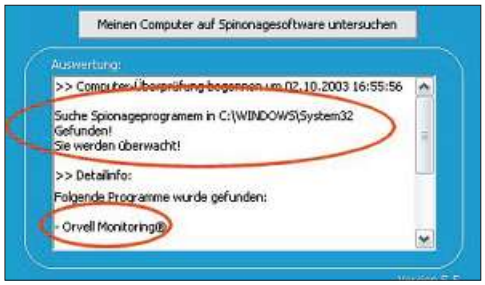
## Spuren lesen

Fährten verwischen ist eine Spezialität der Spy-Tools. Orvell ist beispielsweise ein Meister der Tarnung, und Starr von Iopus löscht beim Herunterfahren sogar verdächtige Einträge aus den MRU-Listen. Dennoch gibt es kein Programm, das unsichtbar in Windows arbeitet.

Erste Anlaufstelle für den Spionage-Check ist der Taskmanager: Der Stealth-Modus der Snooper verhindert nicht, dass sich die Programme im System korrekt anmelden müssen, sofern diese nicht von einem zentralen Server aus gestartet werden. Folglich outet sich jede Spyware im Taskmanager. Zur besseren Übersicht sortiert der Anwender die gelisteten Tasks über die Schaltfläche Benutzer. Spyware wird, wie auch Viren und Würmer, benutzerabhängig gestartet. Bei den Tasks besteht die Aufgabe darin, mögliche Spione aus den regulären Anwendungen herauszufiltern. Das ist mitunter kompliziert, denn die meisten Monitoring-Tools wählen unauffällige Namen für die Startdateien. Protectcom hat den Namen für die Startdatei in Orvell nicht ohne Ironie gewählt. Das File heißt *svdhost.exe*. Die Ähnlichkeit zum generischen Windows-Dienst *svchost.exe* ist kein Zufall. Wer die laufenden Tasks allein über den Namen sortiert, hat kaum Chancen, die Parasiten im System zu finden.

Stößt der User auf mehrere potenzielle Spy-Kandidaten, ist es ratsam, die Funktion der Dateien zu erörtern. Programme, die beispielsweise heimlich eine Online-Verbindung aufbauen, sind grundsätzlich verdächtig. Über den Kommandozeilenbefehl *netstat -o* und den Abgleich der PID stellt der Anwender fest, welche Anwendung aktuell über welchen Port und welches Protokoll nach außen kommuniziert.

Im zweiten Schritt lokalisiert der Anwender das File im System. Zu Tarnzwecken schreiben sich die Start-Dateien der Monitoring-Tools häufig in das *System32*-Verzeichnis. Sortiert der User im Anschluss die Dateiliste im Explorer anhand des Datums, erscheinen verwandte Dateien direkt untereinander. Aus den Datei-Eigenschaften lassen sich weitere Hinweise auf mögliche Observer ziehen. Von Interesse sind vor allem die Angaben zur Firma (Hersteller), zum Produktnamen und dem Zeitpunkt des letzten Zugriffs. Wurde die Datei über mehrere Tage nicht gestartet, handelt es sich definitiv nicht um aktive Spyware. All diese Informatio-



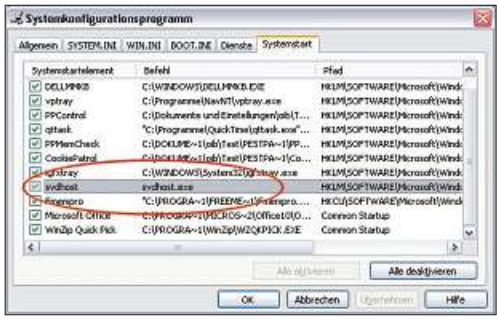

▲ **Treffer: Der Online-Scan von Elbtec hat einen Spion auf der Festplatte entdeckt.**

nen reichen in der Regel bereits aus, um harmlose Programme von Malware zu unterscheiden. Bestehen noch Unklarheiten zum Einsatzzweck eines laufenden Tasks, bietet es sich an, im Web nach weiteren Informationen zu suchen. Dass beispielsweise *svdhost.exe* zur Monitoring-Software Orvell gehört, wissen bereits zahlreiche Webseiten.

## Prozesse & Starteinträge lesen

Profis nutzen den kostenlosen Process Explorer von Sysinternals *(www.sysinternals.com)*, um aktuell laufende Tasks genau im Auge zu behalten. Das Tool protokolliert alle von einem Task ausgehenden Dateizugriffe (Handles) in Echtzeit, verlangt aber vom Anwender enorme Systemkenntnisse, um die DLL- und Registry-Aktivitäten korrekt zu deuten. Ein Monitoring-Tool wird sich unter anderem durch Zugriffe auf zahlreiche Netzkomponenten outen.

Neben den laufenden Prozessen sind vor allem die Startaufrufe von Interesse. Ist eine Überwachungs-Software nicht pausenlos aktiv, erteilt der Taskmanager keine verlässlichen Auskünfte. Viele, aber längst nicht alle Schnüffelprogramme verewigen sich in den Run-Keys der Windows-Registry. Der User sollte nicht nur im Hauptschlüssel *HKEY_LOCAL_MACHINE* nachsehen, sondern auch im benutzerbezogenen Haupt-Key *HKEY_LOCAL_USER*. Einen schnellen Überblick liefert das Tool *Msconfig*, das über den gleichnamigen Befehl in der *Ausführen*-Box gestartet wird. Im Register Systemstart führt Windows die Starteinträge aus allen Quellen zusammen. Wer den jeweiligen Haken löscht, deaktiviert den betreffenden Starteintrag. Außerdem lohnt ein Blick auf die Services im Karteireiter Dienste. In der langen Liste findet sich der Benutzer schneller zurecht, wenn er die Microsoft-Dienste über den entsprechenden Button ausblendet. Aufmerksamkeit verdienen Dienste, die den Hersteller nicht nennen. Hier gilt es, im Web nach weiteren Informationen zu suchen, falls sich das Einsatzgebiet des Services nicht bereits aus dem Namen ergibt. Wenn sich nach eingehender Recherche das Anfangsmisstrauen in einen handfesten Verdacht verwandelt, sollte das Spy-Opfer besonnen bleiben. Unter keinen Umständen ist es erlaubt, die Software auf eigene Faust zu deinstallieren. Im schlimmsten Fall begeht der Benutzer Sabotage und handelt sich eine fristlose Kündigung ein. Statt dessen sollte das Bossing-Opfer sofort den Betriebsrat informieren und – vor Zeugen – den Administrator um Aufklärung bitten.




▲ **Msconfig zeigt einen Dienst, der sich als MS-Service tarnt, aber von einem Monitoring-Tool stammt.**

## Keylogger ausfindig machen

Trotz der geringen Dateimenge und -größe lassen sich Keylogger ebenfalls mit bescheidenen Mitteln enttarnen. Dabei gelten die gleichen Regeln wie für die größeren Spyware-Suiten. Erste Anlaufstellen sind der Taskmanager und Starteinträge im System. Zudem sollte der Anwender nach verdächtigen Logfiles Ausschau halten. Diese tragen in der Regel die Dateiendung *.txt*, *.dat* oder einfach *.log*.

## Professionelle Gegenagenten

Bei der Enttarnung von Spy-Programmen, die beispielsweise anhand von ActiveX-Controls regelmäßig übers Web Daten versenden, ist der Anwender auf professionelle Helfer angewiesen. Pestpatrol *(www.blitzbox.de)* kennt die meisten Keylogger und Monitoring-Tools und hat beim Festplatten-Scan nur wenige Aussetzer. Dass ausgerechnet die aktuellen Versionen von Winston und Orvell dazu gehören, ist allerdings mehr als ein Schönheitsfehler.

Pestpatrol gibt es auch als kostenlosen Online-Scanner unter *www.pestscan.de*. Dieser Festplattencheck ist erstaunlich schnell, die Treffer beschränken sich jedoch auf Malware-Hinweise in bestimmten Verzeichnissen. Außerdem fehlt eine Funktion zum Isolieren oder Löschen der gefundenen Spyware.

Auch Elbtec online *(www.elbtec.de)* hat einen Security-Scanner, der sich auf die Suche nach Monitoring-Tools macht. Das Online-Tool arbeitet in der neuen Version sehr gewissenhaft und meldet auch den »Meister der Tarnung«, Orvell. Davon abgesehen erkennt Elbtec nur noch die Spy-Programme E-Blaster und Spector. Insofern sollte sich der Anwender nicht in Sicherheit wiegen, falls der Online-Scan keinen Treffer meldet. OIB

# LAN im Gefahr

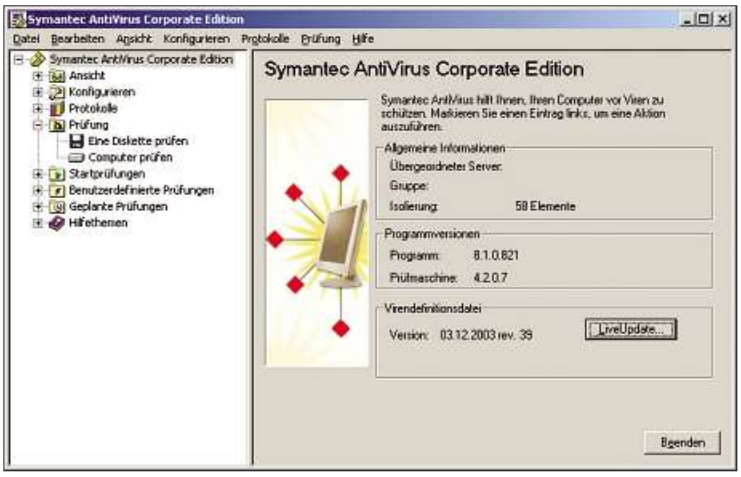
**Würmer bedrohen Server und Netzwerke. Der Artikel zeigt, wie Server-Würmer arbeiten und wie sich Netzwerke davor schützen lassen.**

Martin Goldmann

Desktop-Würmer wie Klez und Fizzer sind in aller Munde und die meisten Anwender wissen sich davor zu schützen. Anders bei Server-Würmern: Dadurch, dass sie direkt die Schaltstelle eines Netzwerks bedrohen – den Server – ist das Gefahrenpotenzial noch höher. Der SQL-Wurm Slammer etwa legte Anfang dieses Jahres im Nu das halbe Internet lahm: Die Sicherheitslücke, die Slammer ausnutzt, ist seit Juni 2002 bekannt. Zahllose Anwender haben versäumt, einen Patch zu installieren, der Slammer unterbindet. Viele Windows-Anwender befürchten jedoch, Microsoft könne bei einem Online-Update Daten auslesen. Doch diese Anwender vergessen dabei, sich um die Sicherheit des eigenen Systems zu kümmern und simple Updates einzuspielen.

## Funktionsweise eines Wurms

Diese Server-Würmer unterscheiden sich von Viren und Trojanischen Pferden. Ein Wurm verbreitet sich selbstständig in Netzwerken. Ein Virus hingegen befällt nur einzelne Computer und vervielfältigt sich nicht eigenständig über das Netz – außer ein Benutzer startet ein von Viren befallenes Programm von einem Netzlaufwerk aus und infiziert so den eigenen Rechner. Das Trojanische Pferd simuliert ein nützliches Programm und trägt meist einen Virus mit sich. Der Wurm braucht also ein Netzwerk, um sich auszubreiten: Das Internet ist prädestiniert dafür.




▲ **Installierte Virenscanner wiegen Administratoren in Sicherheit. Diese Maßnahme allein reicht aber nicht, um ein Netzwerk zu schützen.**

## So schadet ein Wurm

Der Wurm nutzt bekannte offene Ports in Serversystemen, Routern oder Firewalls. Sicherheitslücken in Programmen ermöglichen, Speicherbereiche des Programms zu überschreiben, eigenen Code darin zu platzieren und auszuführen. So auch im Fall von Slammer: Auf einem Server laufen mehrere Dienste, die auf unterschiedlichen Ports Anforderungen abwarten. Der Resolution Service genannte Verteiler, ein Bestandteil von SQL Server nimmt auf Port 1434 Anfragen entgegen und leitet diese an die entsprechenden Instanzen des Servers. Ein Bug in Resolution Service öffnet Slammer das Tor: Slammer kann einen Teil des Speichers mit eigenem Code überschreiben. Der Code an sich ist nicht böswillig, zerstört keine Daten und eignet sich auch nicht, um Denial-of-Service-Angriffe (DoS) auf Server auszuführen. Ebenso wenig öffnet Slammer eine Hintertür, über die Eindringlinge in das System gelangen könnten. Also eigentlich harmlos. Jedoch: Slammer ist auf eine Weiterverbreitung programmiert. Dafür generiert der Schädling automatisch IP-Adressen und versucht diese wieder über den Port 1434 zu erreichen. An die Adressen versendet Slammer einen 376 Byte langen Replikations-Code. Der Server wird wegen der vielen ausgehenden Anfragen überlastet, das Netzwerk kollabiert. Die Abhilfe gegen Slammer ist einfach zu realisieren: Server herunterfahren und rebooten. Somit ist der Wurm entfernt. Zu Beginn der

Slammer-Welle reichte dieses Verfahren allerdings nicht. Zusätzlich musste der Administrator die Ports 1433 und 1434 in den IP-Eigenschaften schließen, damit nicht ein neuer Slammer eindringt. Eine weitere Maßnahme besteht darin, den entsprechenden Patch einzuspielen *(www.microsoft. com/technet)*.

## Unterschiedliche Würmer

Ein anderer Wurm, der Microsoft-Server befällt, ist Code Red, der auf einer bekannten Sicherheitslücke im Index-Server von Microsoft Internet Information Server 4 oder 5 (IIS) basiert. Microsoft hatte schon einen Monat vor dem ersten Code-Red-Angriff einen Patch bereitgestellt, der die entsprechende Sicherheitslücke schließt *(www.support.microsoft.com)*. Auf englischsprachigen Systemen verändert Code Red Inhalte der auf dem IIS gehosteten Webseiten, nicht aber auf deutschen.

Der Wurm W32.Blaster verbreitete sich über einen bekannten Fehler im RPC-Dienst von Windows 2000 und XP. Für Abhilfe sorgt, den Port 135 zu blockieren oder den entsprechenden Patch einzuspielen. Dazu hat Microsoft sogar eine Aktualisierungs-CD veröffentlich, die auch in Ausgabe 11/2003 von *PC Professionell* zu finden war. Nach dem Start der Datei *removal.cmd* wird das Microsoft Sicherheits-Update installiert. Danach wird der PC auf eine Infektion mit dem Blaster-Wurm überprüft. Bei Vorhandensein, wird der Wurm automatisch vom Rechner entfernt.

## Gefahr: die DoS-Attacke

Würmer ebnen auch den Weg für Denial-of-Service-Angriffe. Dabei werden massenhaft Anfragen in manipulierten Paketen an einen Server oder Router geschickt. Aufgrund der Vielzahl von Anfragen kollabiert der Router oder Server. Eine Spezial-Variante der DoS-Angriffe sind Distributed-DoS-Attacken (DDoS). Diese gehen von mehreren Clients aus. Besonders gefährlich sind DDoS-Angriffe für E-Commerce-Seiten: Selbst wenige Minuten offline richten bereits großen finanziellen Schaden an. Auch für lokale Firmennetzwerke ist ein solcher Angriff fatal. Denn liegt der E-Mail-Verkehr brach, ist die Kommunikationsfähigkeit extrem eingeschränkt.

Deswegen muss jeder Administrator die firmeneigenen Router und Server genau prüfen, ob das System ausreichend gegen DoS-Attacken abgesichert ist: Die offenen, jedoch nicht benötigten Ports müssen kontrolliert und gegebenenfalls geschlossen werden.




▲ **Zum Schutz vor dem Blaster-Wurm veröffentlichte Microsoft eigens eine Sicherheits-CD mit dem entsprechenden Patch.**

## Auch Linux-Netze sind nicht frei von Sicherheitslücken

Linux an sich ist zwar sicherer als Windows, doch die zusätzlich mit Linux gelieferten Programme sind nicht frei von Fehlern. So war es in der Samba-Version 2.2.8 möglich, durch einen Programmfehler Root-Zugriff auf das System zu erlangen. Der Schaden, den ein Hacker anrichtet, ist groß, wenn er durch eine unzureichend konfigurierte Firewall eindringt und Malicious-Code in Samba unterbringt. Deshalb sollten Netzwerk-Administratoren unbedingt darauf achten, dass die Firewalls UDP-Port 137, 138 sowie TCP-Port 139 und 445 blockieren. Die Linux-Distributoren bieten nun aktualisierte Software unter *www.samba.org* an.

Zweites Beispiel: Der Wurm Slapper nutzt eine bekannte Schwachstelle in der Sicherheits-Software OpenSSL Version 0.9.6.d und älter. Die ist unter anderem für das Herstellen abgesicherter Verbindungen zwischen dem Webserver und dem Client zuständig. Betroffen sind Linux-Systeme auf Intel-Basis mit Apache-Webserver, die OpenSSL nutzen.

Bei einem Angriff schickt der Wurm zunächst eine ungültige GET-Anfrage an den Port 80. Hat dieser dann anhand der Antwort ein verwundbares System identifiziert, schickt der Wurm über einen anderen Port den gefährlichen Quellcode an das System und versucht daraufhin, sich selbst zu kompilieren. Ist das geschafft, verbreitet sich Slapper selbstständig. Allein der dadurch entstehende Traffic bringt einen Server zum Zusammenbruch. Ebenso lässt sich der Wurm als Basis für Denial-of-Service-Angriffe nutzen oder für den Zugriff auf das System. BBR

# Falsche Fährten

**Spammer beherrschen Tricks, um Mail- und Nachrichtenmüll unter falschen Angaben zu verteilen. Profis enttarnen die Fälschungen über den Mail-Header.**

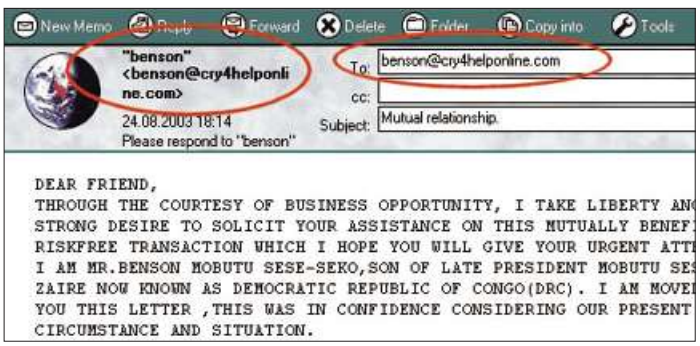
Oliver Ibelshäuser

Spammer bedienen sich immer neuer Tricks, um Massenmails unter falschen Absenderangaben zu verschicken. Spezielle Filterprogramme helfen dem Empfänger, diese Spam-Mails zu erkennen und aus dem Postfach zu entfernen. Wird der Empfänger per Mail persönlich beleidigt oder ist der Verdacht auf eine Straftat gegeben, sollte es der Anwender aber nicht beim Filtern und Löschen belassen, sondern Nachforschungen anstellen, um den tatsächlichen Absender oder zumindest den Provider zu ermitteln. Oftmals reichen Bordmittel, kostenlose Internet-Dienste und das Know-how rund um Mail-Protokolle aus, um bei eingehenden E-Mails auch zwischen den Zeilen zu lesen. Das ist dringend nötig, denn in der Regel sind zahllose Informationen in einer solchen E-Mail gefälscht und gelogen. Das bezieht sich nicht nur auf den reinen Nachrichtentext.

## Verborgene Umschläge von E-Mails

Eine E-Mail enthält wesentlich mehr Informationen als den eigentlichen Inhalt. Neben Body und Header (Adressfeld im Browser) komplettiert der SMTP-Envelope (Simple Mail Transfer Protocol) das Mail-Paket. Dieser nennt den Absender im Klartext sowie den Zielserver. Je nach Mail-Programm wird dieser Umschlag teilweise oder auch komplett beim Eingang der Post entsorgt. Für den fehlerfreien Eingang der Mail ist der SMTP-Dialog allerdings von enormer Bedeutung. Streng genommen handelt es sich dabei um ein Handshake zwischen zwei Servern. Der Ausgangs-Server klopft per *HELO*-Kommando an die Tür, nennt den Absender sowie den Adressaten und übergibt per *DATA*-Befehl die Mail samt Header und Body. Kontrolliert und bestätigt wird dieses Handshake durch Statusparameter, die der angesprochene Mail-Server ausgibt. Beim Anmelden verlangt der Empfangs-Server lediglich eine Absender-Adresse. Im Gegensatz zur IP lässt sich diese aber bequem fälschen. Den Beweis kann jeder User antreten: Über einen Telnet-Aufruf nimmt der Anwender via Standard-Port 25 Kontakt zu einem beliebigen Mail-Server auf. Die Pseudo-Authentifizierung über das Kommando *MAIL FROM* dient allein dazu, dem vermeintlichen Absender mögliche Fehlerberichte zukommen zu lassen. Für den empfangenden Server zählt nur die IP-Adresse. Und selbst die ist in vielen Fällen zunächst nebensächlich, da meistens keine echte Eingangskontrolle stattfindet.

Der Absender spezifiziert den Empfänger über das Kommando *RCPT TO:* Erst jetzt überprüft der Server die Datenanfrage anhand des Adressaten. Akzeptiert der Rechner den Input mit dem Statuscode 250, kann der Absender Header und Body nachreichen. Im Anschluss bestätigt der empfangende Server




**◀ Bei den meisten Spam-Mails sind die sichtbaren Absenderangaben oft schlichtweg gelogen und Empfängerdaten frei erfunden.**

die Zustellung oder Weiterleitung der Mail, und der Absender schließt per *QUIT*-Befehl die Verbindung.

Um nicht als Umschlagplatz für weltweiten Spam zweckentfremdet zu werden, checken die meisten Mail-Server zumindest die IP-Adresse des Absenders umgehend und leiten ausschließlich Mails an berechtigte Empfänger (Mitarbeiter, Kunden oder Mitglieder) weiter. Ein echter Filter ist das nicht, da jede Mail übermittelt wird, sofern nur der Empfänger bekannt ist.

Komplett missbrauchen lassen sich so genannte Open-SMTP-Relays-Server, die alle Mail-Anfragen akzeptieren und in die ganze Welt und an jede Domain ausliefern. Damit gelingt es Spammern, diesen Zugang als Durchgangsschleuse für Mails mit gefälschtem Absender an beliebige Personen zu senden – und zwar tausendfach.




▲ **Ein Mail-Server bestätigt das Versenden einer gefälschten Mail (oben), die unter dem Absendernamen »Bill Gates« zugestellt wird.**

▼




## Echte Spuren, falsche Fährten

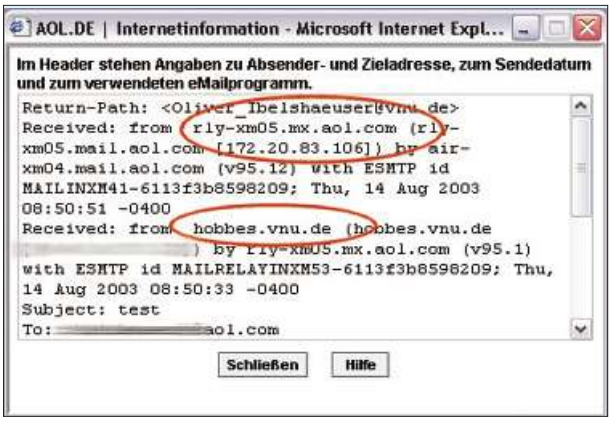
Der Mail-Header ist vergleichbar mit einem Briefkopf und enthält relevante Informationen zum Provider, dem eingesetzten Mail-Programm des Absenders sowie zu den übertragenden Servern (Name und IP-Adresse). Zudem ist immer auch eine Mail- beziehungsweise Message-ID enthalten, die die digitale Post eindeutig klassifiziert. Diese Message-Nummer enthält eine Benutzerkennung sowie das Datum in codierter Form vor dem @-Zeichen und dazu den Rechner- beziehungsweise Host-Namen hinter dem @-Zeichen. Die ID stellt das absendende Programm aus. Verfremdet wird diese normalerweise bis zur Zustellung nicht mehr. Liegt keine Message-ID vor, wie beispielsweise bei einer manuellen Telnet-Attacke, erzeugt der Server, der die Botschaft weiterleitet, diese ID stellvertretend. In dem Fall kennzeichnet die Nummer die Mail zwar noch immer eindeutig, lässt aber keinerlei Rückschlüsse mehr auf den eigentlichen Verfasser zu. Entgegen der landläufigen Meinung sind die meisten Infos im Header nicht fälschungssicher. Beispielsweise findet der User unvermittelt eine Mail in seinem Postfach, die scheinbar an jemand anders gerichtet ist. Das kommt bei Massenmailings sehr häufig vor und lässt sich schnell auflösen. Allein die Eingabe zum Empfänger (Recipient) im Envelope gibt an, auf welche Reise eine Mail geht.

Die Infos im Header sind demgegenüber vor allem für die Anzeige im Mail-Client wichtig. Aus diesem Grund sucht das Spam-Opfer hin und wieder die eigene Adresse im Header vergeblich. Um in dem Telnet-Beispiel zu bleiben: Die Absender-Adresse, die im Outlook- oder Notes-Fenster erscheint, lässt sich über eine *MAIL FROM:*-Anweisung von Hand eingeben. Eine Domain-Kontrolle oder -Zuordnung findet nicht statt. Insofern ist auch die Zeile *Return-Path* im Header einer Mail mit Vorsicht zu genießen.

## Reiseroute von E-Mails

Lässt man einmal mögliche Manipulationen außer Acht, protokollieren die Header-Daten den Weg, den eine E-Mail auf dem Weg zwischen Absender und Empfänger zurücklegt. Die einzelnen Stationen sind mit einem Zeitstempel versehen und lassen bei einer verzögerten Zustellung vage Rückschlüsse auf den Verursacher zu. Eine Manipulation dieser Nennungen ist unwahrscheinlich, aber nicht ausgeschlossen.

Zu Beginn des Headers steht der Return-Path, ein Feld, das das Mail-Programm normalerweise setzt. Allerdings könnte auch ein Benutzer Hand anlegen. Die oberste (in seltenen Fällen auch unterste) Received-Zeile entspricht dem Eingangsstempel beim eigenen Provider oder Mail-Server. Die Angaben sind korrekt, führen in der Regel jedoch lediglich zum vorletzten Überbringer in der mitunter langen Kette der Mail-Zusteller. Jeder Server-Eintrag in der Received-Reihe




▶ Der Ausgangsstempel kennzeichnet den Absender-Server (unten), der Eingangsstempel nennt den Überbringer und den empfangenden Server (oben).

weist auf seinen Zusteller hin und nennt den nächsten Empfänger. Der Ausgangsstempel befindet sich im untersten Received-Vermerk. Das sind die Informationen, die der aussendende Mail-Server einträgt. Ist diese logische Kette unterbrochen, verrät das eine Manipulation des Headers.

Je nach Mail-Programm und Übertragungsart findet der Anwender hinter der Received-Zeile zwei Server-Nennungen. Die Erste ist meist die des Umschlags, die Zweite ist jene, die der empfangende Server über die IP eigenständig ermittelt hat. Diese Reihenfolge ist aber nicht zwingend. Sind beide Angaben gleich, liegt kein Täuschungsmanöver vor. Andernfalls ist grundsätzlich den Angaben des empfangenden Mail-Servers zu trauen, der sich nicht austricksen lässt. Folgt statt einer Wiederholung des Servers lediglich die IP-Adresse, ist das ein Indiz dafür, dass eine eindeutige Zuordnung nicht möglich war. Aus den Received-Zeilen lassen sich unter Umständen ebenfalls persönliche Informationen des Absenders auslesen – etwa dessen Mail-Provider sowie der Rechnername. Etwa ist das Protokoll qmail häufig ein Hinweis auf den Provider *Gmx.t-dialin.net* und besagt, dass sich der Anwender über T-Online ins Internet einwählt. Folgt hinter dem *HELO*-Kommando ein Name, ist das meist die PC-Bezeichnung.

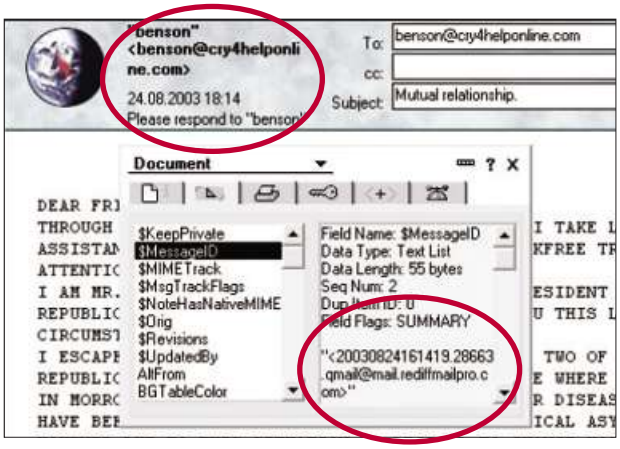
Übrigens: Hin und wieder findet sich im Header eine Kommentarzeile, die dem Absender über Einträge wie Authenticated- oder X-Sender den Status »vertrauensvoll« geben soll. Diese Angaben müssen nicht gelogen sein, definitiv wahr sind diese aber auch nicht. Alle Zeilen, die mit »X« beginnen, lassen sich manuell oder von einem Tool einfügen. Zeitstempel geben vage Rückschlüsse auf den Server-Standort. Nicht selten nehmen innerdeutsche Mails den Umweg über amerikanische Server, wie etwa bei AOL. Allerdings deuten mehrere Minuten dauernde Zeitsprünge nicht unbedingt auf technische Probleme hin. Die Server sind nämlich nicht auf die gleiche Zeit geeicht. Nur wenn der Mail-Eingang am Ziel-Server von der Weitergabe in das User-Postfach stark abweicht, liegt vermutlich ein Netzwerk-Problem vor.

## Der Forward-Trick

Die Message-ID wird für den Durchlauf bis zum digitalen Post-Einwurf beibehalten. Danach aber wird sie verworfen, selbst wenn die gleiche Mail anschließend noch an Hunderte weiterer Adressaten geht. Beim Weiterleiten legt der Server eine neue ID an, weil es sich um eine neue Zustellung handelt. Dabei gehen die ursprünglichen Received-Informationen verloren, was sich leicht überprüfen lässt: Der Anwender schickt eine Mail, die im Büro-Postfach gelandet ist, an seinen privaten Web-Account bei Hotmail oder AOL weiter. Die Internet-Eigenschaften weisen nur noch die letzten Überbringer aus, von dem ersten Versand fehlt jede Spur. Dieses Prinzip nutzen Spammer zuweilen aus, um über einen »parkenden Host« Spuren zum eigenen Rechner auszumerzen.

## Remailer, Proxys und Remixer

Nach einem ähnlichen Prinzip, wenn auch deutlich professioneller, arbeiten Remailer. Deren Aufgabe ist es, die Spuren des Users zu vernichten. Wie von Proxy-Servern bekannt, geht es dabei vor allem um die Tarnung der IP-Adresse. Eine Verschleierung ist vor al-




▲ Die Message-ID enttarnt den tatsächlichen Absender-Server (unten) im Gegensatz zur Angabe im Browser (oben).

lem dann zweckmäßig, wenn der User eine Standleitung mit fester IP-Zuordnung einsetzt und über einen POP3-Account mailt. Webmailer wie Freenet oder Web.de übertragen hingegen die IP-Adresse des Provider-Servers. Der User bleibt zwar nicht anonym, die zweifelsfreie Identität lässt sich aber nur vom Provider feststellen.

Professionelle Remailer benutzen eine ganze Kette von Proxy-Servern als Zwischenstationen. Absenderangaben werden dabei vernichtet, die Empfängeradresse vorübergehend verschlüsselt, um Manipulationen auf dem Übertragungsweg auszuschließen. Je nach Anbieter wechseln die Postboten mehrfach. Hinderlich: Ist einer der Server down, geht die Mail verloren, weil eine Lagerung oder Rücksendung im späten Stadium der Weitergabe technisch nicht mehr möglich ist.

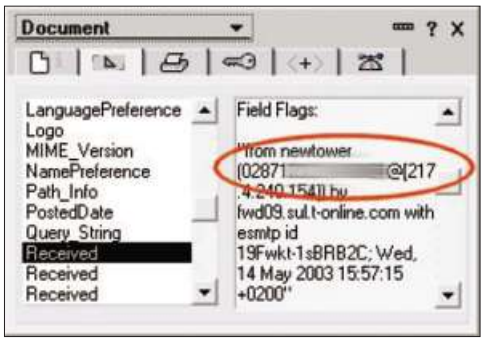
Viele Spammer suchen sich Webdienste in Ostasien. Wer mehr als fünf Proxys hintereinander reiht, hat gute Chancen, unerkannt zu bleiben, zumal es eine internationale Strafverfolgung bislang nicht gibt.

## Spam-Mails zurückverfolgen

Wird der Anwender regelmäßig von Spam geplagt, die immer die gleiche Handschrift trägt, erscheint es durchaus sinnvoll, der Sache auf den Grund zu gehen. Die nötigen Werkzeuge hat der User bereits an Bord oder findet diese im Internet. Die volle Identität des Angreifers lässt sich freilich nicht offen legen. Garantiert aber findet der Benutzer heraus, ob es sich um eine manipulierte Mail handelt, welche Server und Provider benutzt wurden und aus welchem Land die Botschaft stammt. Beim Verdacht auf eine Straftat ist allerdings Strafanzeige zu erstatten.

Erster Anhaltspunkt sind die Received-Zeilen. Stößt der Anwender bei der Kontrolle nach den oben genannten Kriterien auf Ungereimtheiten, weil beispielsweise der Absender nicht genannt wird oder der Name des Senders von der Browser-Angabe abweicht, liegt eine manipulierte Mail vor. Die oberste Received-Zeile enthält das Empfangs-Protokoll des eigenen Servers samt Daten zum Überbringer. Interessanter ist jedoch der letzte Received-Eintrag, der den Absender und dessen IP zeigt. Hieraus liest der Anwender meist, dass es sich um Webmail (via http) oder SMTP handelt. Im ersten Fall führen die Nachforschungen zum Webmail-Anbieter im Internet. Im zweiten Fall führt die Rückverfolgung über die IP zum Mail-Server am Arbeitsplatz des Absenders. In diesem Fall ergibt sich der Firmenname meist aus der Domain. Hat der in der Mail-Kette an nächster Position stehende Server keine automatische IP-Zuordnung vorgenommen, holt das der User nach. Über den Kommandozeilenbefehl *nslookup* plus IP-Adresse löst der Anwender die Zahlenkolonne in eine Domain auf.

Um eine Fälschung auszuschließen, wird die Kontrolle wiederholt, indem aber nun die Domain aufgelöst wird. Dazu dient das Kommando *traceroute*. Werkzeuge wie Traceroute, aber auch Whois und Nslookup findet der Anwender als Online-Tools unter *www.haferbeck.de/tool*. Übersichtlich zeichnet auch *visualroute.visualware.com* die Route bis zu einem gewünschten Mail-Server nach. OIB




◀ **T-Online-User hinterlassen im Mail-Header meist unfreiwillig die eigene Telefonnummer im Klartext.**

Sie // Sabrina will Dich // haben // I love you // neue E-Mails // Wann war der Termin? // erhalten.
MDaemon Mailserver mit AntiSpam, AntiVirus und GroupWare. Online unter: www.mdaemon.de

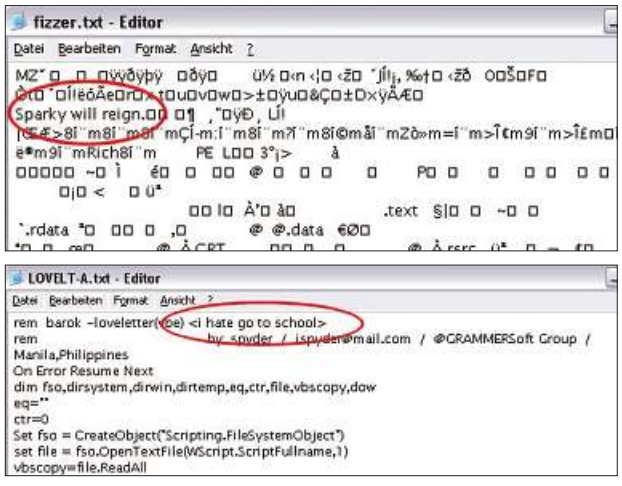
eulink*

# Tarnen & Täuschen

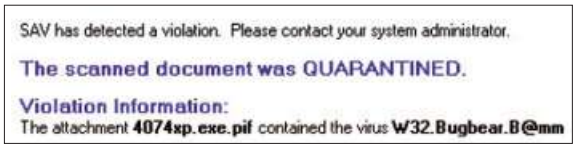
**Viren tarnen sich meist mit unverfänglichen Dateiformaten, die keinen Angriff vermuten lassen. Profi-Tools demaskieren solche bösartigen Programme.**

Oliver Ibelshäuser

Mehrere Millionen Anwender weltweit erhielten in den letzten Monaten Post von Microsoft. Bill Gates höchstpersönlich verschickte eine Support-Mail, mit dem Hinweis, eine Sicherheitslücke per angefügter Datei schließen zu wollen. Statt eines Patches enthielt diese jedoch den Virus Sobig-C, der sich schlagartig ausbreitete und es im Juni 2003 mit rund zehn Prozent aller Infektionen nach Bugbear auf Platz zwei der internationalen Viren-Hitlisten schaffte. Die Gründe für den Siegeszug des Massen-Mailers: Vermeintliche Nachrichten von Microsoft wecken selten Misstrauen beim Anwender, und die wenigsten User vermuten hinter seltenen Dateiformaten gefährlichen Code. Während angehängte EXE-Dateien und VBS-Programme per se als verdächtig gelten, rutschen PIF-, HTA- oder SCR-Dateien durch das Sicherheitsraster. Aktuelle Virenscanner lassen sich von der Maskerade normalerweise nicht überlisten, sofern diese mit aktuellen Signaturen über ein Online-Update vom Anwender regelmäßig gepflegt werden.




▶ **Virenautoren verewigen sich häufig im Programm – oben »Sparky« im W32-Virus Fizzer, unten »Spider« im VBS-Virus Loveletter.**




◀ **Bösartiger Code: Die PIF-Datei beherbergt den W32-Virus Bugbear.**

## PIF & SCR: Wirte für Viren

Auch Bugbear kommt dieser Tage als PIF-Datei – häufig mit einer Doppel-Extension – per Mail. PIF steht für Program Information File und bezeichnet einen von Microsoft eingeführten Standard, der eigentlich für Verknüpfungen zu DOS-Dateien zuständig ist. Windows XP beherrscht noch immer den Umgang mit dem eigentlich ausgestorbenen Format dank des PIF-Managers *pifmgr.dll*.

Zwei Dinge machen PIFs für Virenautoren interessant: Erstens verbirgt Windows die Endung standardmäßig, und zweitens starten PIF-Dateien automatisch nach einem Doppelklick. Wer nun aufgrund des alten Formats annimmt, darin verpackte Viren hätten nur ein begrenztes Schadensrepertoire, irrt. Der nur rund 250 KByte große Fizzer ist einer der gefährlichsten Viren des Jahres 2003 und tritt ebenfalls als PIF-Datei auf. Dieser Massen-Mailer protokolliert auch Tastatureingaben und späht persönliche Dokumente aus.

Ebenfalls weit oben auf der Indexliste verdächtiger Extensions steht SCR. Ursprünglich allein für Screensaver vorgesehen, sind SCR-Dateien auch in der Lage, beliebigen bösartigen Code zu transportieren und nach Doppelklick auf dem System auszuführen.

## Weitere Datenformate

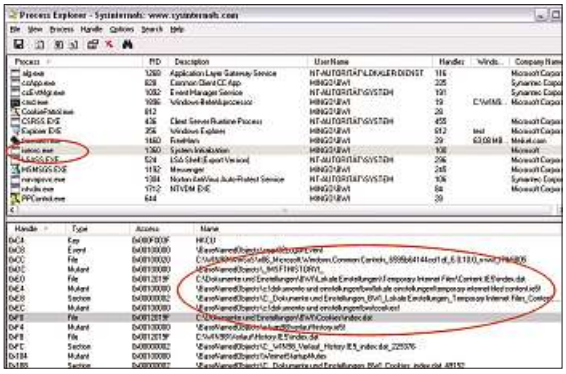
Auch andere Formate haben sich als Viren-Transporteure einen Namen gemacht: Vorsicht ist vor allem beim Öffnen von Skripts geboten, die als VBS-Files oder Javascripts (JS) per Mail kommen. Diese Dateien sollten vor dem Aufruf zunächst lokal gespeichert und von einem Virenscanner kontrolliert werden. Selbst in Mails eingebundene HTML-Files oder deren Links bergen letztlich Gefahren,

da die Datei respektive die verlinkte Seite im Web ebenfalls gefährlichen Code bereitstellen oder automatisch einen Download vollziehen kann. Einen sehr guten Überblick zu gefährdeten Dateitypen finden Anwender auch auf der Webseite *www.bandpromo.de/home/viren/viren2.html*.

## Professionelle Datenanalyse

Empfangen Anwender per Mail Dateien mit einer Doppelendung, gibt es nur eine Empfehlung: sofort löschen. Wer dabei die [Umschalt]-Taste drückt, verschiebt die Datei nicht nur in den Papierkorb. Für reinrassige PIF-, SCR- oder VBS-Dateien gilt diese Regel ebenfalls. Daneben stößt der Anwender auch auf Zweifelsfälle – etwa bei komplett unbekannten Dateitypen. Umsichtige User beauftragen zunächst den Virenscanner mit der Inspektion der Daten. Um letzte Zweifel auszuschließen, empfiehlt sich die Analyse der Bits und Bytes. Zunächst speichert der Anwender die verdächtige ausführbare Datei auf der Festplatte. Um die Gefahr einer Virenifektion durch einen versehentlichen Doppelklick auszuschließen, konvertiert der Anwender das File, indem er die bestehende Extension mit TXT überschreibt. Nun lässt sich die Datei gefahrlos öffnen. Erste Anlaufstation ist dafür ein Text-Editor wie etwa Notepad.

Die Datei zeigt auf den ersten Blick kilobyteweise Maschinencode. Dennoch finden sich auch eindeutige Spuren, die eine Malware ausweisen. Viele Virenautoren haben die Angewohnheit, sich im Programm zu verewigen. Im Massen-Mailer Fizzer entdeckt der User bereits in den ersten Zeilen die Ankündigung »Sparky will reign«. Im letzten Drittel der Datei stehen die vom Programm benötigten Kommandos für bestimmte APIs sowie die erforderlichen Bibliotheken. Befehle, die neue Services starten (Beispiel: *RegisterServiceCtrl*) sowie gehäufte Registry-Aufrufe (Beispiel *RegCreateKey*), verdienen auf jeden Fall erhöhte Aufmerksamkeit. Einen sehr guten Überblick zu der Auswirkung zahlloser Kommandos liefert die MSDN-Library unter *(msdn.microsoft.com/library/default.asp)*. Eine deutschsprachige Übersicht zu den häufigsten API-Kommandos gibt die Seite *www.activevb.de/rubriken/apikatalog/bylib/bylib121.html*. Übrigens: Am Schluss der Datei sammeln sich zahlreiche Informationen zum Hersteller und zur Version. Diese können durchaus gefälscht sein. Das gilt aber nicht für den Namen der Startdatei, die ein vermeintliches Virenprogramm erzeugt und in der Übersicht ebenfalls auftaucht.



◀ **Der Virus Fizzer fragt persönliche Einstellungen ab und manipuliert Dateien.**

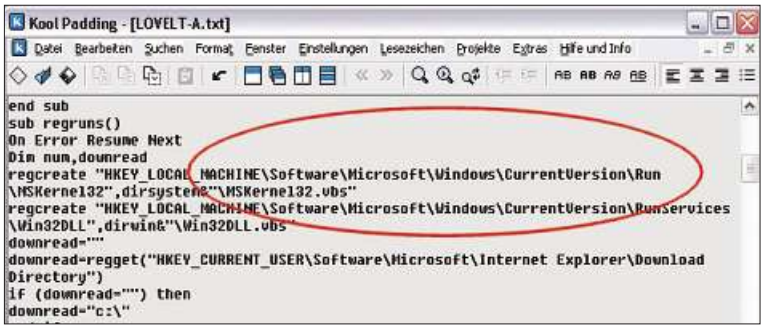
## Warnsignal: integrierte SMTP-Funktion

Erhärtet sich der Verdacht, eine unbekannte Datei beherberge einen Virus, sucht der Anwender zudem nach Massen-Mailer-Spuren. Dazu gehören vor allem eingebettete SMTP-Engines, die die Vervielfältigung per Mail automatisch übernehmen. Neben Outlook & Co sollte in der Regel kein Programm die Erlaubnis haben, eigenmächtig Nachrichten zu verschicken. Bei Würmern wie Nimda findet der Anwender eine Reihe eindeutiger Hinweise, etwa Erklärungen zum Mime-Header oder dem Content-Typ. Diese Begriffe tauchen im Programmcode auf. Bei anderen Viren wie beispielsweise Klez wird der Anwender fündig, wenn er nach den Zeichenketten »smtp« oder »Mail to« sucht.

## Leichtes Spiel mit Skript-Viren

Eine vergleichsweise dankbare Aufgabe ist das Enttarnen von Skript-Viren in Form von Makroviren, Javascripts oder VBS-Dateien. Das gilt auch für HTA-, HTM- und HMTL-Files, die ebenfalls Skripts enthalten können.

Zur Information: HTA bezeichnet eine HTML-Applikation, die ebenso viel gefährlichen Code enthalten kann wie eine EXE-Datei. Speichert der User die Files wiederum als TXT-Dateien und öffnet diese danach im Editor, erscheinen die Anweisungen als Plain Text. Die Vorgehensweise fast aller Skript-Viren ist letzten Endes ähnlich: Über Routinen stellt das Programm fest, ob es bereits geladen wurde. Dann verankert der Virus eine infizierte Datei im System, meist ein Skript im gleichen Format, sorgt dann dafür, dass diese Datei automatisch geladen und per Mail an beliebige Adressen weiter versendet wird. Insofern zeigen die Code-Segmente mehrere verdächtige Spuren, die Profis sofort ins Auge springen. Registry-Einträge gehören dazu. Zum Beispiel setzen sich viele Skript-Viren




**Der Freeware-Editor Kool Padding demaskiert einen VBS-Virus über einen neuen Eintrag im Run-Key. Über diesen Eintrag werden die Virenaktivitäten gestartet.**

im *Run*-Key fest, benennen System-Dateien um und benutzen veränderte Systemeinstellungen für Outlook Express im Registry-Ordner. Typischerweise nehmen Skript-Viren eine Adressbuchabfrage über den Key *Hkey_Current_User\Software\Microsoft\wab* vor.

Tipp: Für die Suche nach verdächtigen Strings gibt es komfortablere Editoren als Notepad, die auch mehrere Dateien öffnen und deren Inhalt vergleichen. Gute Dienste leistet die Freeware Kool Padding *(www.koolpeople.de)*. Der Editor bietet etwa ein paralleles Editieren mehrerer Texte, eine erweiterte Zwischenablage, das Ersetzen von Textstrings in mehreren Dateien gleichzeitig sowie ein Datei-übergreifendes Suchen.

## Hex-Editor: Dateien entschärfen

Nicht immer reicht ein einfacher Editor aus, um den Programmcode studieren zu können, da etwa Notepad nur wenige Zeichensätze beherrscht. Unbekannte Zeichen wie Trennelemente übersetzt der Editor nicht korrekt. Das ist unübersichtlich. Authentisch ist dagegen die Darstellung in Hex-Editoren. Zudem ermöglichen diese ein exaktes Bearbeiten der Files, etwa das Löschen oder das Extrahieren verdächtiger Strings auf Bit-Ebene. So lassen sich ausgewählte Programmsegmente separat starten und überprüfen. Das ist aber nur Profis zu empfehlen.

Vor allem für die Analyse unbekannter DAT- und BIN-Files sollte der User den Hex-Editor jedem Text-Editor vorziehen. Beide Extensions stehen allerdings nicht unbedingt für Viren. Das gilt auch für nicht kompilierte Dateien. Auf einschlägigen Seiten werden im Internet aber gerade diese Formate für den Transfer gefährlicher Viren benutzt, weil die Scanner bei ihnen in der Regel nicht anschlagen. Fragen zu unbekannten File-Formaten beantwortet die Seite *www.filext.com*.

Zu den empfehlenswerten Hex-Editoren mit einer Fülle an professionellen Funktionen zählt Winhex. Eine funktionseingeschränkte Version des Tools steht auf der Seite *www.winhex.com* zum Download bereit. Das Tool bietet Zugriff auf die Daten, die andere Programme verstecken. Zu den Features zählen ein Diskeditor, ein RAM-Editor zum Editieren des virtuellen Speichers anderer Windows-Programme und ein Daten-Dolmetscher für 20 Datentypen. Damit ist es möglich Datenstrukturen mit Schablonen zu editieren, zu verketten, zu zerlegen, zu analysieren und zu vergleichen. Dabei helfen die flexiblen Suchen- und Ersetzen-Funktionen. Zudem können Anwender Zwischenablage-Formate inklusive Hexwerte im Textformat importieren und in andere Formate konvertieren.

## Verborgene Aktivitäten aufspüren

Auch bei einer sorgfältigen Prävention können Fälle auftreten, in denen Programme mit Malicious Code starten. Dazu reicht ein versehentlicher Doppelklick aus. Schlägt der Virenscanner nicht an, bedeutet das nicht automatisch Entwarnung: Malware, neue Viren und vor allem Backdoor-Programme rutschen auch verlässlichen Sicherheitslösungen hin und wieder durch. Programme, die Windows in Tasklist oder Systray darstellt, machen nur einen Bruchteil der tatsächlich laufenden Anwendungen, Dienste und Threads aus. Beispielsweise versucht auch der Windows Messenger ständig, sich heimlich im System anzumelden. Malware-Programme führen ohnehin alle Aktivitäten im Hintergrund aus.

Zunächst kontrollieren Anwender laufende Prozesse über den Taskmanager unter Prozesse. Dort werden auch der Benutzer und vor allem die Prozess-ID (PID) genannt – beide sind für die Identifizierung von Malware wichtig. Relevant sind aber nur Einträge, die dem aktuellen Benutzer zugeordnet werden. Systemprozesse sind meist integer. Taucht ein verdächtiger Task in der Liste auf, überprüft der User erst, ob die Anwendung Kontakt zur Außenwelt aufnimmt. Dazu gibt er den Kommandozeilenbefehl *netstat -o* in der Eingabeaufforderung ein. Windows stellt nun alle aktiven Verbindungen des Hosts samt Port-Be-

legung dar. Wird eine ungewollte Kommunikation erkennbar, ist diese umgehend über den Taskmanager zu beenden.

Als gefährlich gelten hierbei Direktverbindungen (TCP oder UDP) zu unbekannten Servern. Hohe Port-Belegungen sind dabei ein typisches Anzeichen von aktiven Backdoor-Programmen und Trojanern. Da auch *netstat -o* die PID einblendet, ist die Identifizierung der betreffenden Anwendung im Taskmanager unproblematisch möglich.

### Professionelle Analyse

Diese Vorgehensweise ist nur eine Erste-Hilfe-Maßnahme beim Verdacht auf eine Datenattacke. Für eine Detailanalyse setzen User spezielle Tools wie etwa den Process Explorer von Sysinternals *(www.sysinternals.com)* ein. Die Freeware listet wahlweise Registry-Handles oder DLL-Zugriffe auf. Praktisch: Auf Wunsch lassen sich einzelne Zugriffe oder komplette Tasks mit einem Mausklick beenden. Geübte User sind in der Lage, die Aktionen beliebiger Anwendungen in Echtzeit zu verfolgen und unter Umständen zu stoppen. Letzteres gilt aber nur für Programme, die sich sowohl in den Start-Einträgen der Registry verewigen, die persönlichen Ordner des Benutzers durchwühlen und Zugang zu Internet-Anwendungen erhalten möchten.

Mit der Shareware Process Manager *(www.efsoftware.de)* können User aktive Prozesse und Anwendungen anzeigen – auch diejenigen, die der Taskmanager nicht kennt. Wahlweise lassen sich alle geladenen Module anzeigen oder nur solche, die von bestimmten Prozessen benutzt werden. Die Ergebnisse der Analyse können für die spätere Aufbereitung als Text und Tabelle exportiert werden.

Gleichermaßen nützlich und hilfreich ist demgegenüber der Registry-Monitor Regmon, der ebenfalls von Sysinternals stammt. Das Programm protokolliert zuverlässig die Registry-Zugriffe laufender Anwendungen. Diese Funktion erfolgt in Echtzeit.

Zur Systemkontrolle empfiehlt es sich, wenigstens einmal pro Woche entsprechende Logfiles anzulegen und die Liste nach verdächtigen Registry-Aufrufen abzusuchen. Das Tool DLL Show *(www.gregorybraun.com)* zeigt eine Liste mit allen aktiven Prozessen sowie deren Abhängigkeiten von DLL-Dateien und ermittelt ausgiebige Informationen über die verschiedenen Prozesse: Name, ID-Nummer, Priorität, Versionsnummer, Anzahl der davon abhängigen Anwendungen und das entsprechende Installations-Verzeichnis des jeweiligen Prozesses. OIB

## Überblick – seltene & gefährdete Dateiformate

| Extension | Beschreibung | Malcode-Gefahr[1)] | Empfehlung[1)] |
|---|---|---|---|
| $$$ | Temporäre Datei | – | – |
| 386 | Ältere Win-Gerätetreiber | – | – |
| ABK | Corel-Draw-Sicherheitskopie | – | – |
| APP | Windows-fremde Applikation | – | – |
| ARC | Archivdatei | mittel | Kontrolle durch Virenscanner vor und nach Entpacken |
| ARJ | Archivdatei | mittel | Kontrolle durch Virenscanner vor und nach Entpacken |
| ASC | Textdatei | – | – |
| ASM | Assembler-Datei | gering | Kontrolle durch Code-Abgleich |
| ASP | Skript Active Server Page | mittel | Kontrolle durch Virenscanner und Code-Abgleich |
| ASP | Stapelverarbeitungsdatei | gering | Kontrolle durch Virenscanner und Befehlsabgleich |
| BIN | Quellcode-Datei | – | – |
| C | C-Datei | – | – |
| C++ | C++-Datei | – | – |
| CAB | (Windows-)Archivdateien | gering | Kontrolle durch Virenscanner vor und nach Entpacken |
| CFG | Konfigurationsdatei | gering | Kontrolle durch Code-Abgleich |
| CGI | Skriptdatei | gering | Kontrolle durch Virenscanner und Code-Abgleich |
| CMD | OS/2-Datei | – | – |
| COM | Programmdatei | hoch | Kontrolle durch Virenscanner und Code-Abgleich |
| CSS | Stylesheet-Datei | – | – |
| DAT | Datendatei | – | – |
| DBF | DBase-Datei | – | – |
| DCR | Shockwave-Datei | – | – |
| DCX | Makrodatei | gering | Kontrolle durch Virenscanner |
| DLL | Programmbibliothek | mittel | Kontrolle durch Virenscanner |
| DOC | Word-Datei | mittel | Kontrolle durch Virenscanner |
| DOT | Word-Template | hoch | Kontrolle durch Virenscanner und Code-Abgleich |
| DRV | Treiberdatei | – | – |
| DTD | XML-Definitions-Datei | gering | – |
| EXE | Programmdatei | hoch | Kontrolle durch Virenscanner |
| GZ | Unix-Datei | – | – |
| HLP | Hilfedatei | gering | Kontrolle durch Virenscanner und Code-Abgleich |
| HTA | HTML-Datei | hoch | Kontrolle durch Virenscanner und Code-Abgleich |
| HTM | HTML-Datei | mittel | Kontrolle durch Virenscanner und Code-Abgleich |
| HTML | HTML-Datei | mittel | Kontrolle durch Virenscanner und Code-Abgleich |
| ICO | Windows-Icon | – | – |
| INF | Installationsanweisungen | – | – |
| INI | Initialisierungsdatei | – | – |
| JS | Javascript-Datei | hoch | Kontrolle durch Virenscanner und Code-Abgleich |
| LHA | Archivdatei | mittel | Kontrolle durch Virenscanner vor und nach Entpacken |
| LIB | Library-Datei | – | – |
| LNK | Verknüpfung | – | – |
| LZH | Archivdatei | mittel | Kontrolle durch Virenscanner vor und nach Entpacken |
| MDB | Access-Datei | – | – |
| NFO | Textdatei | – | – |
| OCX | ActiveX-Control | gering | Kontrolle durch Virenscanner und Code-Abgleich |
| PCX | Bilddatei | – | – |
| PDF | Adobe-Format | – | – |
| PIF | Programmverknüpfung | hoch | Kontrolle durch Virenscanner und Code-Abgleich |
| PNG | Bildformat | – | – |
| PPS | Powerpoint-Präsentation | – | – |
| PS | Postscript-Datei | – | – |
| PST | Outlook-Datei | – | – |
| RAR | Archivdatei | mittel | Kontrolle durch Virenscanner vor und nach Entpacken |
| REG | Registrierungsdatei | hoch | Abgleich der Registry-Einträge |
| RTF | Textdatei | – | – |
| SCR | Screensaver | hoch | Kontrolle durch Virenscanner und Code-Abgleich |
| SWF | Flash-Datei | mittel | Kontrolle durch Virenscanner |
| SYS | Systemdatei | mittel | Kontrolle durch Virenscanner |
| TAR | Linux-Archiv | gering | – |
| TIF | Bilddatei | – | – |
| TMP | temporäre Datei | gering | – |
| VBS | Skriptdatei | hoch | Kontrolle durch Virenscanner und Code-Abgleich |
| VXD | virtueller Gerätetreiber | – | – |
| XML | XML-Datei | gering | Kontrolle durch Virenscanner |
| XLS | Excel-Datei | mittel | Kontrolle durch Virenscanner |
| XLT | Excel-Datei | hoch | Kontrolle durch Virenscanner |
| ZIP | Archivdatei | mittel | Kontrolle durch Virenscanner vor und nach Entpacken |

[1)] Der Gedankenstrich » – « bedeutet, dass keine akute Virengefahr besteht. Eine Empfehlung gibt es daher nicht.

# Malicious XML

**XML als Plattform-übergreifendes Austauschformat birgt neue Gefahren. XML-Firewalls und modifizierte Virenschutztechnik sorgen für Sicherheit.**

Bettina Weßelmann

Die Metasprache XML ermöglicht einen einfachen Informationsaustausch zwischen heterogenen Applikationen. Neben eigens programmierten Webservices, bei denen In- und Output primär über XML-Dokumente abgewickelt werden, können auch traditionelle Anwendungen mit vorgeschalteten Konvertern XML-fähig gemacht werden. Oft geschieht dies zum Beispiel bei Datenbanksystemen, die speziell für ein Unternehmen programmiert wurden und seit Jahren in Betrieb sind. Endanwendern begegnet XML immer häufiger als Dateiformat von Office-Paketen.

## Neue Sicherheitsprobleme

XML bringt aber auch Gefahren mit sich, die von klassischen Security-Lösungen nicht vollständig abgewehrt werden können. Das erste große Sicherheitsproblem von XML ist der Code selbst: Fehlerhafte Anweisungen – etwa ein Start-Tag <*Printdaten*>, zu dem das End-Tag </*Printdaten*> fehlt, oder ein Attribut, das einen für die Anwendung bekömmlichen Wertebereich überschreitet – können einen Webservice genauso zum Absturz oder Stillstand bringen wie eine klassische Datenbank. Ein Hacker könnte also auch per XML versuchen, etwa mit ungewöhnlichen Werten oder Steuerzeichen in Eingabezeilen, Abstürze oder falsche Ergebnisse zu provozieren.

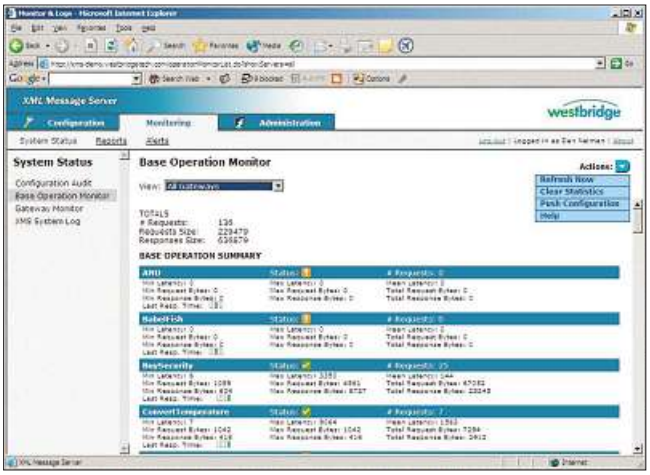



Bild Westbridge

**▲ Die Oberfläche der Westbridge-XML-Firewall: Anschauliches Monitoring für den Administrator erleichtert die zentrale Abwehr von XML-Gefahren.**

## Flexibilität schafft Angriffspunkte

Die Zahl der Möglichkeiten, XML-Code fehlerhaft zu handhaben oder bewusst zu missbrauchen, ist aufgrund der Flexibilität der Metasprache hoch. Die Extensible Markup Language sieht zwar ähnlich aus wie HTML, ist aber nicht auf einen festen Satz von Tags beschränkt. Sie lässt sich mit immer neuen Elementen ausstatten, die von den Anwendungen ausgewertet werden. Als Elemente gelten dabei Tags mit den dazwischen eingebundenen Inhalten. XML erlaubt es, auf der Basis dieses Grundmusters nicht nur Text-, Layout- und Grafikinhalte, sondern auch Anweisungen zu transportieren. So genannte Parser in den Anwendungen übernehmen die Aufgabe, den XML-Content zu interpretieren. Selbst die Steuerung von Produktionsmaschinen ist auf diese Weise möglich.

Eine erste wichtige Sicherheitsmaßnahme für Webservices besteht deshalb in der Prüfung, ob zu verarbeitende XML-Dokumente gültig und wohlgeformt sind. Als wohlgeformt gilt eine XML-Datei dann, wenn ihre Elementnamen aus gültigen Zeichen bestehen, die Start- und End-Tags symmetrisch zueinander passen, Attribute richtig deklariert wurden und die Datei ein so genanntes Root-Element enthält, eine Klammer aus Start- und End-Tag, die das gesamte Dokument umfasst und bezeichnet. Als gültig wird ein XML-Dokument dann bezeichnet, wenn sein Inhalt mit der Strukturbeschreibung übereinstimmt, die der Datei entweder in Form einer Document Type Definition (DTD) beigegeben wird oder in Form eines XML-Schemas.

Beide Verfahren dienen dazu, Namen von Elementen und Attributen sowie Datentypen und Wertebereiche anzugeben. Mit der Prüfung, ob hier Wertüberschreitungen und Unstimmigkeiten vorliegen, wird die Gefahr von DoS-Angriffen über unerlaubte XML-Funktionen reduziert. Das Fehlen von Abweichungen im Dokumentinhalt von vorher getroffenen Festlegungen gibt außerdem eine gewisse Sicherheit, dass die Datei nicht von Dritten verändert wurde.

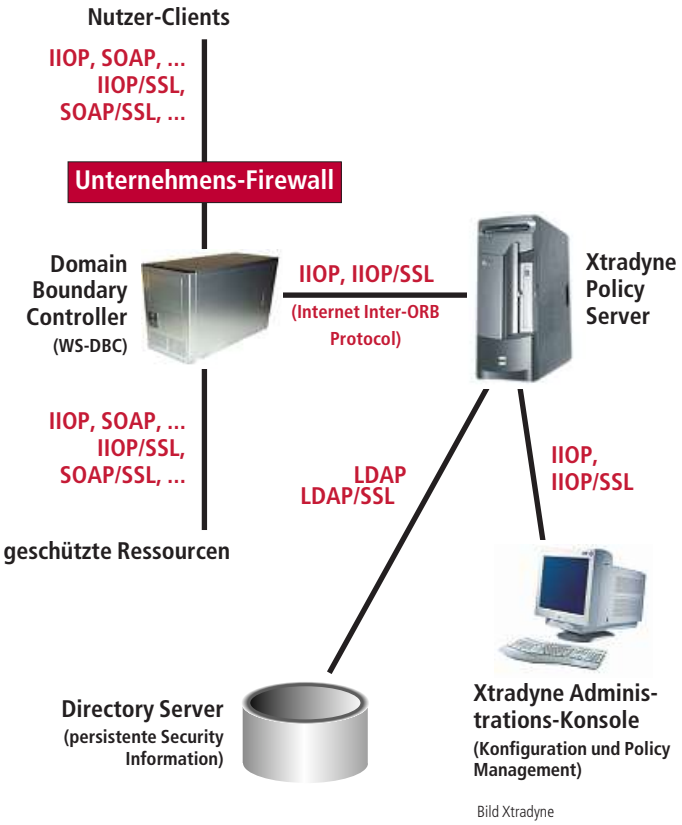
## Spezialisierte Firewall-Technik

Die Prüfung auf Gültigkeit und Wohlgeformtheit zielt auf rein formale Eigenschaften eines XML-Dokuments. Sie kann deshalb gut am Übergang zu einer Webservices-Umgebung von spezialisierten Software- oder Hardware-Lösungen mit entsprechenden Parsing-Fähigkeiten übernommen werden. Die Produkte müssen zusätzlich zum Simple Objects Access Protocol (Soap) kompatibel sein, denn Soap wird dazu gebraucht, XML-Inhalt für die Informationsübertragung durchs Web wie in einem Umschlag in gewöhnliche HTML-Dateien zu verpacken.

Firmen wie Westbridge *(www.westbridgetech.com)*, Reactivity *(www.reactivity.com)* und Quadrasis *(www.quadrasis.com)* haben Unternehmens-Gateway-Lösungen für die XML-Kontrolle unter der Bezeichnung XML-Firewalls auf den Markt gebracht. Die spezialisierten Content-Scanner nehmen eine Wächterstellung an der Grenze zu einer Unternehmens-Infrastruktur ein, beispielsweise als Proxy in der Demilitarisierten Zone (DMZ). Während beim klassischen Netzwerk-Traffic anhand der Port-Adresse und Paketform unterschieden werden kann, ob man es beispielsweise mit Daten für FTP-, Web- oder Spezialanwendungen zu tun hat, besteht diese Möglichkeit beim XML-Konzept nicht mehr. Firewalls herkömmlicher Technologie können deshalb zwar noch zur Sicherung einer XML- und Webservices-Umgebung beitragen, indem sie einzelnen Systemen im Netz anhand ihrer IP-Adresse das Senden oder Empfangen von XML-Daten erlauben oder verbieten. Die eigentlichen Gefahren aber stecken im Content auf der Application-Layer-Ebene.

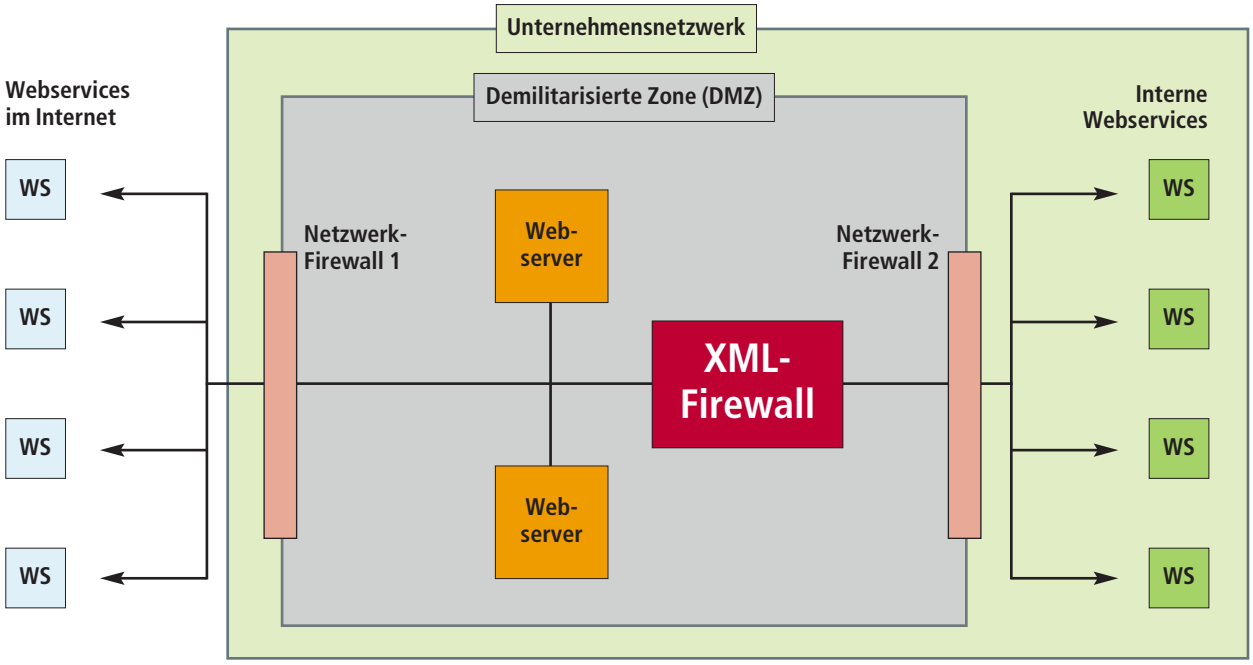
## Kein Ende der Virengefahr

Die zweite Problematik, die im Zusammenhang mit dem XML-Einsatz für die Informationssicherheit entsteht, ist eine neue Variante bekannter Gefahren: Webservices-Infrastrukturen haben wie traditionelle Netze mit




▲ **Die XML-Firewall WS-DBC von Quadrasis/Xtradyne arbeitet mit einem Richtlinien-Server und einem LDAP-Verzeichnisdienst zusammen.**

Viren zu kämpfen. Denkbar sind speziell geschriebener XML-Code, der selbst Abstürze oder Berechnungsfehler provoziert, und eingebundene ausführbare Sabotageprogramme. Aber auch bekannte Viren dürften vom neuen Transportmedium XML Gebrauch machen, da sich hinter manchem Webservice ja eine traditionelle Anwendung in einer XML-Schale verbirgt. Prinzipiell bilden wieder die XML-Firewalls den Ansatz zur Abwehr, da sich in deren Parsing-Technik auch Virenscanner einbinden lassen. Außerdem bieten die Produkte die Möglichkeit, potenziell gefährlichen Inhalt zentral per Sicherheitsrichtlinie abzublocken. Dass dem Problem nicht einfach beizukommen ist und dass auch die Produkte für Endanwender angepasst werden müssen, zeigt das Beispiel Microsoft Office 2003. Virenscanner konnten bisher immer sehr schnell ermitteln, ob beispielsweise eine Excel- oder Word-Datei überhaupt aktive Elemente enthielt und deshalb auf Makroviren geprüft werden muss. Bei den neuen XML-Dokumentformaten gelingt dies nicht – hier muss der Virenschutz die gesamte Datei durchkämmen, um Malicious Code zu entdecken. So könnte ein Engpass im Bereich des Viren-




▲ **Integration ins Unternehmens-Netz: Die XML-Firewall in der DMZ kontrolliert, was den Netzwerk-Firewalls entgeht. Die traditionelle Firewall-Technik schützt weiter die Client-Server-Anwendungen.**

scanners auftreten, der zu einer Denial-of-Service-Attacke geradezu einlädt: Bereits mit genügend XML-Kommunikation ließe sich das Mailsystem einfach in die Knie zwingen.

## Authentifizierung am Gateway

Zentral für XML-Sicherheit – und ebenfalls eine Aufgabe für XML-Firewalls am Gateway – sind schließlich auch Authentifizierung und Autorisierung. Im Fall von Webservices müssen sich nicht nur die Anwender gegenüber den Programmen ausweisen, sondern auch die Webservices untereinander. Es geht nicht nur darum, ob ein XML-Dokument etwa von einem Partnerunternehmen kommt, das Input senden darf, sondern zusätzlich darum, ob beispielsweise ein Buchhaltungsdienst auch mit dem richtigen Bestellservice im eigenen Unternehmen kommuniziert. In den XML-Traffic muss somit starke Authentifizierung und Autorisierung mit Zertifikaten, PKI und Verschlüsselung in die XML-Technik eingebaut werden können – mit all der Komplexität einer vollen PKI-Integration, rollengestütztem Single Sign-on oder unter Umständen auch den Lücken eines einfachen Sender-Kennwort-Systems, wie sie außerhalb der XML-Welt bekannt sind. Die Elemente und Tags für diese Sicherheitsaspekte sind zu XML-Untersprachen wie SAML (Security Assertion Markup Language) oder WS-Security zusammengefasst worden, die die Verwendung in XML regeln. Firmen wie RSA Security *(www.rsasecurity.com)* und Verisign *(www.verisign.de)* bieten Kryptotechnik, Sicherheitsserver und Managementhilfen zur Umsetzung an. Prinzipiell funktioniert die Einbindung von Authentifizierungs- und Autorisierungsdaten wie mit beliebigen anderen Elementen auch: So könnte ein XML-Dokument einen verschlüsselten Text, eine digitale Unterschrift oder ein Zertifikat und den öffentlichen Schlüssel des Absenders enthalten.

Maßnahmen zur Abwehr von XML-Gefahren müssen derzeit vor allem Unternehmen treffen, während Endanwender auf ein Update ihrer Virenscanner warten können. Für die Corporate-Netze sind XML-Firewalls mit zentraler Sicherheitsadministration die beste Lösung. Die einzige Alternative – der Einbau aller Sicherheitsfunktionen in die einzelnen Anwendungen – würde eine schwer zu verwaltende, inhomogene Security-Infrastruktur entstehen lassen. Wer nach Sicherheitslücken in seiner Webservices-Umgebung suchen will, findet dazu mit Webinspect von SPI Dynamics *(www.spidynamics.com)* einen spezialisierten Vulnerability-Scanner.

Die Chancen stehen damit gut, dass sich XML als neues universelles Dokumentformat und Webservices als Basis einer neuen Unternehmensinfrastruktur so durchsetzen können, wie es sich die Anwender erhoffen. Bisher haben vor allem die Sicherheitsprobleme diese Entwicklung behindert. HME

# XP-Verschlüsselung

**Mit dem Encrypting File System verfügt Windows XP über ein Werkzeug, das vertrauliche Dateien und Verzeichnisse sicher verschlüsselt.**

Oliver Ibelshäuser

Zu den Sicherheits-Highlights von Windows XP gehört das Encrypting File System (EFS), das sich sehr einfach anwenden lässt. Hat der User Administratorenrechte auf einer NTFS-Platte, so genügen zwei Mausklicks, um eine Datei zu schützen. In den Eigenschaften eines Ordners klickt der Anwender auf den Button *Erweitert* und im Dialog *Erweiterte Attribute* auf *Inhalt verschlüsseln*. In der folgenden Box kennzeichnet der Benutzer, ob die Verschlüsselung nur für diesen Ordner gelten soll oder auch für darunter liegende Ebenen samt aller Dateien – was in der Regel empfehlenswert ist.

## So funktioniert EFS

Der komplexe Prozess des Ver- und Entschlüsselns ist für den Nutzer zunächst unsichtbar. Meldet sich ein Anwender mit seinem Passwort an und öffnet einen entsprechend geschützten Ordner, so entschlüsselt Windows XP die Daten automatisch und unverzüglich im Hintergrund. Genau genommen besitzen die geschützten Ordner und Dateien lediglich ein weiteres, verstecktes Attribut (»E«). Für das Verschlüsseln benutzt EFS ein Schlüsselpaar – einen öffentlichen und einen privaten Schlüssel sowie einen weiteren Key für jede einzelne Datei (»Verschlüsselungsschlüssel«). Diesen so genannten File Encryption Key (FEK) verschlüsselt Windows XP mit dem öffentlichen Schlüssel des Benutzers (asymmetrisches Verfahren) und legt diesen gemeinsam mit der Datei ab. Der FEK entspricht dabei einer Zufallszahl und ist immer einzigartig. Die erforderlichen Zertifikate erzeugt Windows XP – falls das erforderlich ist – selbst, so dass der Anwender keinen Konfigurationsaufwand hat. EFS setzt immer ein NTFS-Volume voraus. Codiert werden dabei entweder einzelne Dateien oder ganze Ordner. Als irreführend erweist sich hier, dass Windows XP optisch einen kompletten Ordner als verschlüsselt kennzeichnet, obwohl sich darin beispielsweise nur eine einzige EFS-Datei befindet. Nur bei Offline-Dateien verschlüsselt Windows stets den gesamten Pool.

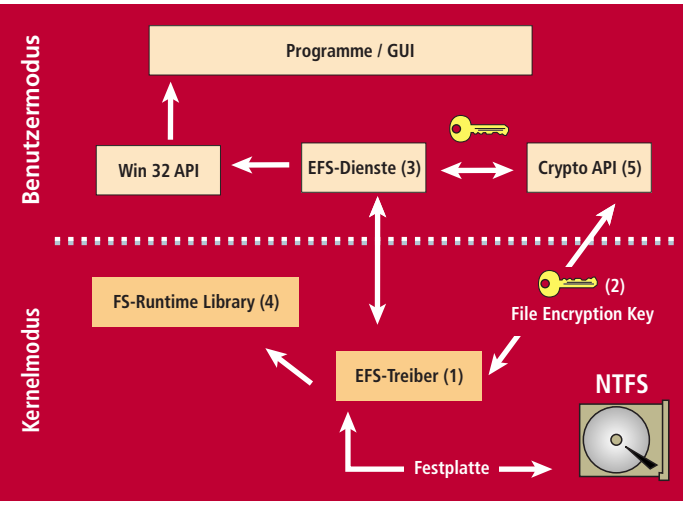
**Über den versteckten Windows-Dialog verschlüsselt der Anwender beliebige Ordner in wenigen Schritten.**




## Komponenten von EFS

Das verschlüsselnde Dateisystem besteht aus einer Reihe eng miteinander verknüpfter Komponenten, die für die Kommunikation zwischen Kernel, Filesystem und Anwendungen sorgen. Direkt auf dem Dateisystem NTFS liegt der EFS-Treiber als grundlegende Ebene der Verschlüsselung. Der Treiber informiert den EFS-Dienst und fordert Verwaltungsdienste an. Dieser EFS-Dienst wiederum ist Teil des Sicherheits-Subsystems in XP. Seine Aufgaben sind das Generieren von Daten-Entschlüsselungsfeldern (Data Decryption Fields, DDF), Daten-Wiederherstellungsfeldern (Data Recovery Fields, DRF) und die Protokollierung der File Encryption Keys (FEKs). Zur Kommunikation mit dem EFS-Treiber werden bestehende Informationskanäle (Local Procedure Call, LPC) verwendet. Hat der Treiber die erforderlichen Daten eingeholt, so werden diese samt den FEKs an die File System Run Time Library (FSRTL) weitergeleitet. Dabei handelt es sich um eine Bibliothek, die im Verborgenen Dateiaufgaben wie Schreiben oder

## Zentrale EFS-Komponenten




◀ Auf der Kernel-Ebene holt der EFS-Treiber (1) den File Encryption Key (2) und Verschlüsselungsfelder von den EFS-Diensten (3) ein. Außerdem füttert der Treiber die FS Run Time Library (4), die sich um das Datei-Handling der verschlüsselten Files kümmert. Die Verschlüsselung selbst geschieht im Benutzermodus. Von dort aus kommuniziert der EFS-Dienst (3) nicht nur mit dem EFS-Treiber, sondern auch mit der Crypto-API (5), die sämtliche Aufgaben der Verschlüsselung übernimmt (Schlüssel generieren, Schlüssel speichern, Schlüssel verteilen). Außerdem übernimmt der EFS-Dienst den Datentransport für die Win-32-API (6), die anderen Anwendungen verschlüsselte Dateien zur Verfügung stellt.

Öffnen erledigt. Die Verschlüsselung selbst läuft nicht mehr im Kernel-Modus ab, sondern im User-Mode. Dort greift das EFS auf die Crypto-API (Crypto Application Programming Interface) zurück. Diese Programmier-Schnittstelle enthält weit reichende Kryptographie-Funktionen, die diese anderen Anwendungen zur Verfügung stellt. So nutzen beispielsweise Anwendungen von Drittanbietern die Crypto-API, um Verschlüsselungen durchzuführen. Zuständig ist die API auch für die Code-Signatur sowie für das Erstellen und Speichern der Schlüssel. Fordert eine andere Anwendung eine verschlüsselte Datei an, so muss die Erlaubnis vom EFS-Dienst erteilt werden, bevor das File über die Win-32-API geöffnet werden kann. Das Entschlüsseln übernimmt das EFS im Speicher.

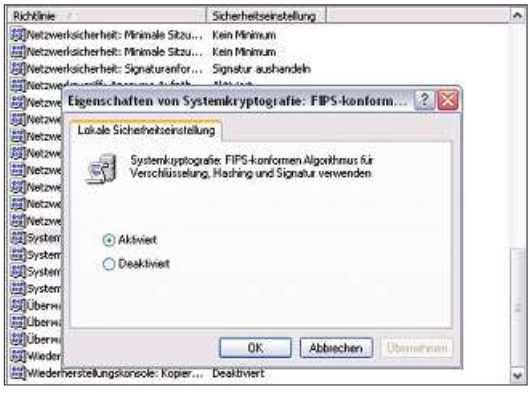
### Chronologische Verschlüsselung

Die Zusammenarbeit der Komponenten vollzieht sich stets chronologisch nach einem festen Muster. Gibt der Anwender über das Kontextmenü den Auftrag zur Verschlüsselung, startet das EFS zunächst eine Prüfroutine. Diese fragt ab, ob das File bereits verschlüsselt ist, ob es sich um eine Systemdatei handelt, deren Codierung unter Umständen verboten ist und ob ausreichend Ressourcen für die nachfolgenden Schritte zur Verfügung stehen. Ergibt der Check keine Probleme, dann übergibt der Treiber das Kommando an den EFS-Service. Dieser fordert einen Schlüssel für die Dateiverschlüsselung von der Crypto-API an und codiert diesen mit dem öffentlichen Schlüssel des angemeldeten Users. Im Anschluss verfügt das EFS über die Metadaten wie Daten-Entschlüsselungsfeld (DDF) und Daten-Wiederherstellungsfeld (DRF). Zudem speichert das EFS auch den Verschlüsselungs-Algorithmus ab.

Zur Codierung der Ausgangsdatei erzeugt Windows XP zunächst ein temporäres File, das jedes Bit aus der Quell-Datei übernimmt. Ist der Vorgang beendet, löscht Windows alle Bits im Ausgangs-File, indem das Betriebssystem die Länge des Datastreams auf Null setzt. Das Quell-File selbst bleibt jedoch physikalisch bestehen. EFS übergibt die Metadaten und kennzeichnet damit die leere Datei als verschlüsselt. Die Verschlüsselung der Bits findet statt, während Windows XP die Daten aus der Temp-Datei zurückschreibt. Danach prüft das EFS, ob der Schreibvorgang korrekt verlaufen ist, und löscht die temporäre Datei.

### Kommandozeilenbefehl Cipher

Dieses Verfahren birgt mitunter die Gefahr, dass unverschlüsselte Datenreste auf der Platte zurückbleiben, wenn etwa die geschriebenen Daten nicht komplett in einen Datensatz der Master File Table (MFT) hinein-




◀ Eine versteckte Einstellung in den Gruppenrichtlinien aktiviert den 3DES-Algorithmus für das gesamte System.

passen. Windows XP hat dafür den Kommandozeilenbefehl *cipher.exe* von Windows 2000 (SP 1) übernommen. Zusammen mit dem Parameter *W* löscht Cipher auf dem gesamten Volumen alle Daten, die von Windows als nicht verwendet gekennzeichnet sind – eine empfehlenswerte Option für Anwender, die häufig Daten verschlüsseln. Ganz sicher geht hingegen, wer zu verschlüsselnde Dateien zunächst in einem bereits geschützten Ordner anlegt. Diese erhalten automatisch das Attribut »E«. In diesem Fall landen definitiv keine Datenreste auf der Festplatte, da Windows XP keine temporären Zwischenlager benötigt. Das Tool ver- und entschlüsselt Dateien und Ordner über bestimmte Parameter und generiert auch nach Bedarf neue Dateiverschlüsselungsschlüssel. Wichtige Parameter lauten *E* für die Verschlüsselung, *D* für die Entschlüsselung und *K* für das Anfordern eines neuen Verschlüsselungsschlüssels. Über den DOS-Befehl */?* zeigt Cipher alle verfügbaren Parameter an.

### (A)symmetrische Verfahren & 3DES

EFS basiert auf einer Kombination unterschiedlicher Verfahren und Schlüssel, um ein »Knacken« geschützter Files mit größtmöglicher Sicherheit zu verhindern. Das Schlüsselpaar aus öffentlichem und privatem Key wird vom Basiskryptographie-Dienstanbieter (CSP) angefordert, der in Windows XP implementiert ist. Öffentliche Schlüssel erfordern immer asymmetrische Verfahren. Das bedeutet, dass ein Programm oder ein Betriebssystem eine Datei mit unterschiedlichen Schlüsseln codiert. Einer dieser Keys (der private Schlüssel) ist anwendergebunden, der andere (der öffentliche Schlüssel) frei verfügbar – etwa im Netzwerk. Bei dem symmetrischen Verfahren ist das Schlüsselpaar identisch, was eine deutlich geringere Codierzeit mit sich bringt.

EFS beherrscht und nutzt beide Varianten. Der FEK maskiert Dateien und Ordner über das symmetrische Verfahren, um eine möglichst hohe Verarbeitungsgeschwindigkeit zu gewährleisten. Windows XP codiert je nach Einstellung mit dem Triple-DES-Verfahren. DES steht für Digital Encryption Standard und wurde 1977 von der National Security Agency (NSA) eingeführt. Ursprünglich arbeitete DES mit einer Schlüssellänge von 56 Bit, aktuell mit einer maximal 168 Bit langen Verschlüsselung – daher der Name Triple-DES.

Allerdings muss der Anwender diesen Standard selbst aktivieren. Dazu öffnet er in der Management-Konsole (Snap-in: *Gruppenrichtlinie*) den Eintrag *Computerkonfiguration/Windows-Einstellungen/Sicherheitseinstellungen/LokaleRichtlinien/Sicherheitsoptionen*. Im rechten Fenster genügt ein Doppelklick auf den Eintrag *Systemkryptographie*. Im folgenden Dialog setzt der Anwender ein Häkchen vor *Aktiviert* und schließt das Fenster mit *Übernehmen*. Den FEK selbst schützt Windows asymmetrisch. Der öffentliche Schlüssel dazu stammt aus dem Zertifikat für öffentliche Schlüssel. Diese Informationen speichert Windows im Header einer jeden geschützten Datei. Zur Entschlüsselung nimmt XP den umgekehrten Weg: Zunächst wird der FEK mit dem privaten Schlüssel ausgelesen. Der FEK selbst gibt dann den Datei-Inhalt frei. Da die verschlüsselten FEKs an-

## EFS-Verschlüsselungsverfahren




**◀ Der FEK verschlüsselt die Datei symmetrisch, also mit einem identischen Schlüsselpaar. Den FEK selbst verschlüsselt das EFS im Anschluss asymmetrisch. Den öffentlichen Schlüssel (grün) speichert Windows frei zugänglich. Der private Schlüssel (gelb) ist an den User-Account gebunden.**

wendergebunden sind, ist die Zahl der FEKs für jede Datei so groß wie die Zahl der Anwender mit Zugangsberechtigung.

## Schlüssel und Zertifikate verwalten

Zu den EFS-Vorzügen von Windows XP gehört die Mehrbenutzerfähigkeit. Über den Button *Details* in den *Erweiterten Attributen* einer Datei stößt der User auf die Verschlüsselungsdetails. Dort listet Windows XP sämtliche Anwender auf, die Zugang zu diesem File haben. Auf diesem Weg findet der User auch das eigene Zertifikat. Beim Setzen eines Zertifikats sucht EFS zunächst im persönlichen Zertifikatsspeicher des Anwenders. Führt dieser Weg nicht zum Erfolg, fahndet EFS etwa im LAN nach verankerten Zertifizierungsstellen. Erweist sich auch dieser Weg als Sackgasse, erzeugt das EFS selbst ein Zertifikat samt beider Schlüssel über die Crypto-API. Den öffentlichen Codierungs-Schlüssel hinterlegt Windows im Zertifikat des Benutzers, den privaten Codierungs-Schlüssel zum Decodieren im Benutzerprofil.

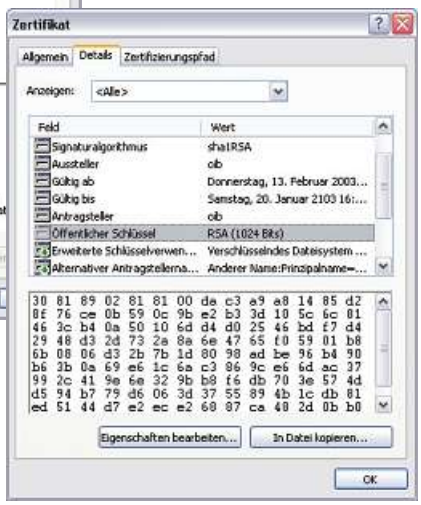
Neue Zertifikate können über die Management-Konsole und das passende Snap-in *Zertifikate* geladen werden. Dazu öffnet der User über das Kommando *mmc.exe* die Konsole und lädt das Snap-in. Schneller kommt der Anwender mit dem Eingabebefehl *certmgr.msc* ans Ziel. Windows listet unter *Eigene Zertifikate* einen oder mehrere Einträge auf, die für den Anwender gültig sind. Ist der Adressat (»Ausgestellt für«) mit dem Absender (»Ausgestellt von«) identisch, handelt es sich um ein selbst signiertes Zertifikat. Externe Zertifikate erhält der Benutzer, indem er im linken Fenster den Eintrag *Zertifikate* mit der rechten Maustaste anklickt und im Kontextmenü den Befehl *Alle Tasks/neues Zertifikat anfordern* wählt. Dafür muss der Verzeichnisdienst Active Directory eingerichtet sein. Ist ein weiteres Zertifikat lokal oder im Netz vorhanden, hat der User zudem die Möglichkeit, dieses über den Menübefehl *Alle Tasks/Importieren* einzuspielen.

## Sicherheitslücken und -risiken

EFS unter Windows XP ist sicher. Das Verschlüsselungsverfahren ist mit vertretbarem Aufwand nicht zu knacken, solange der User die EFS-Spielregeln einhält. Ein Risiko besteht, dass sich der Anwender selbst aussperrt, etwa wenn er ein Benutzerkonto löscht oder einen privaten Schlüssel zerstört. Der Key liegt als versteckte (und verschlüsselte) Datei im Unterordner *RSA* innerhalb des Pfads *Dokumente und Einstellungen*. Eine sichere Wiederherstellung der Daten gewährleistet in einigen Fällen der Wiederherstellungs-Agent von Windows XP, der zuvor über die Domäne als Gruppenrichtlinie konfiguriert werden muss.




◀ **Das vom EFS selbst erzeugte Zertifikat wird als nicht vertrauenswürdig gekennzeichnet – eine irreführende Mitteilung.**




**Das lokal erstellte Zertifikat zeigt den öffentlichen Schlüssel zum Decodieren der Datei. ▶**

Unter Sicherheitsaspekten sinnvoll ist der Export des privaten Schlüssels auf ein externes Medium samt Kennwortschutz. Das erledigt der Anwender über das Snap-in *Zertifikate*. Dort reicht ein rechter Mausklick auf den Zertifikateintrag und die Wahl des Befehls *Alle Tasks/Exportieren*. Im Anschluss hilft ein Datenwiederherstellungs-Agent bei der Rekonstruktion der Files.

Zu einer häufigen Fehleinschätzung trägt Windows XP selbst bei: Befindet sich eine verschlüsselte Datei in einem Ordner, so kennzeichnet Windows XP den kompletten Ordner farbig. Das Betriebssystem suggeriert damit, alle darin enthaltenen Files seien geschützt. Das ist jedoch nur der Fall, wenn zuerst ein codierter Ordner angelegt wird und darin anschließend die Dateien erzeugt oder alle Files der Reihe nach verschlüsselt werden. Probleme gibt es auch beim Einsatz von Antiviren-Software, die den verschlüsselten Content nicht prüfen kann. Auch bei einem Backup sollte der Anwender prüfen, ob die Verschlüsselung vom jeweiligen Programm übernommen werden kann. Letztlich steht und fällt die EFS-Sicherheit mit der Sicherheit in Windows XP: Wer Zugang zum System erlangt, kann dort wahllos Daten manipulieren und löschen. OIB

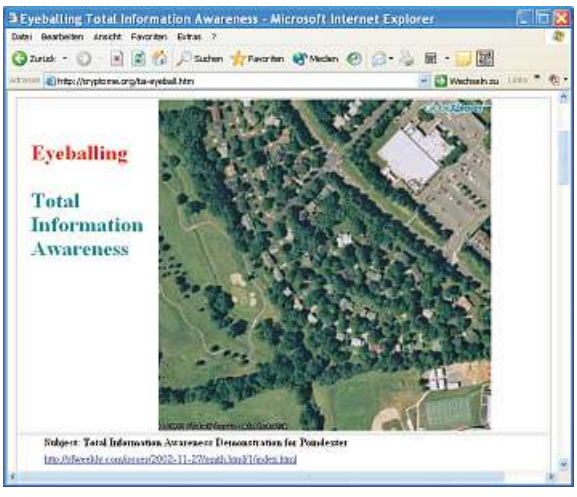
# Nie allein im Web

**Zu den Weggefährten von Internet-Surfern zählen Spione, Betrüger und Saboteure. Besonders gefährlich: so genannte Social-Engineering-Attacken.**

Bettina Weßelmann

Eine neue Klasse von Internet-Übeltätern begeht im großen Stil Identitätsdiebstahl. Damit kaufen die Täter mit fremden Kreditkarten ein oder betreiben Industriespionage. Eine andere Variante ist die Auftragssabotage, um einer bestimmten Firma Wettbewerbsvorteile zu verschaffen. Das Tun der Angreifer bleibt häufig unbemerkt. Eines ihrer wichtigsten Instrumente hierbei ist das Social Engineering. Diese Methode arbeitet nach dem Prinzip, mit einmal recherchierten Informationen über eine bestimmte Person oder Institution in mehreren Schritten weitere Informationen zu sammeln. Schließlich hat der Angreifer genug Daten, um die Zielperson entweder zu manipulieren, zu betrügen, zu bestehlen oder für ein anderes kriminelles Vorhaben ihre Identität anzunehmen.

Im Gegensatz zum Hacker will der Social Engineer vertrauliche Informationen am Ende nicht mit einem Hacker-Trick erlangen, sondern sein Opfer dazu bringen, ihm die Daten freiwillig zu überlassen. Dabei nutzt er immer wieder den Effekt, dass Detailwissen Vertrauen erweckt: Wer beispielsweise genau weiß, welche Position eine bestimmte Person in einem Unternehmen einnimmt, wie ihre Abteilung im internen Jargon heißt, welche Namen ihre Kinder haben und wen der Betreffende am vergangenen Wochenende besucht hat, wird es leicht haben, als scheinbarer Freund aufzutreten und dem Mitarbeiter weitere Informationen zu entlocken.




**Social Engineering gegen Staatsspionage: Hacker haben Adresse und Luftaufnahmen der Villa John Poindexters ins Web gestellt, dem Leiter des Programms Total Information Awareness.**

## Spurensuche im Web

Die direkte Kommunikation mit dem Opfer oder ihm nahe stehenden Personen ist der Endpunkt der Social-Engineering-Kette. Am Anfang der Informationssammlung stehen meist technische Verfahren, die auf Internet-Recherchen und dem Einsatz spezieller Tools beruhen. Der Großteil dieser Methoden ist dabei sogar legal. Der Angreifer versucht nämlich nur, verstreute Daten besonders geschickt aufzuspüren und zueinander in Beziehung zu setzen. Dieses Vorgehen müssen Internet-Nutzer kennen, um sich gegen entsprechende Attacken wehren zu können.

Zusammen genommen ergibt sich aus vereinzelten Informationen schnell ein aussagekräftiges Profil: E-Mail-Adresse und Internet-Verbindung, postalische Adresse und wichtige Details wie Arbeitsplatz, Laufbahn, Beruf sowie persönliche Vorlieben. Wissenschaftler und Selbstständige sind darüber hinaus oft in öffentlichen Spezialdatenbanken eingetragen. Für den Social Engineer sind persönliche Details seines Opfers entscheidend, um es erfolgreich zu kontaktieren, nicht technische Daten.

Der Übergang in die rechtliche Grauzone erfolgt, sobald Informationen nicht mehr mit legalen Such-Tools erlangt werden. Hat sich über die öffentlichen Informationen etwa ergeben, dass eine Person über einen bestimmten Provider ans Internet angeschlossen ist oder bei einem bekannten Unternehmen arbeitet, wird Social Engineering möglicherweise wieder zum Hacking. Der Angreifer verwendet dann illegale Tools, um schlecht gesicherte Details aus geschützten

Netzen zu erlangen. Eine Privatperson mit ihrer Kreditkarte und ihren Gehaltskonten ist selten wichtig genug für eine Attacke. Aber jeder Mensch ist über sein Arbeitsverhältnis potenziell ein wichtiges Glied in der Informationsbeschaffung eines Industriespions. Für einen Mittelständler irgendwo auf der Welt, der günstige Haushaltsgeräte für Europa produzieren will, kann es äußerst lukrativ sein, auf die Projektdatenbank eines Konkurrenten vor Ort zuzugreifen. Immerhin ist dieser nah am Kunden und weiß deshalb, was gerade verlangt wird, muss aber teurer produzieren. Dass so wenige Fälle von Industriespionage bekannt werden, liegt nicht daran, dass diese nicht stattfinden: Viele Betroffene merken einfach nichts davon, und die übrigen verschweigen den peinlichen Vorfall.

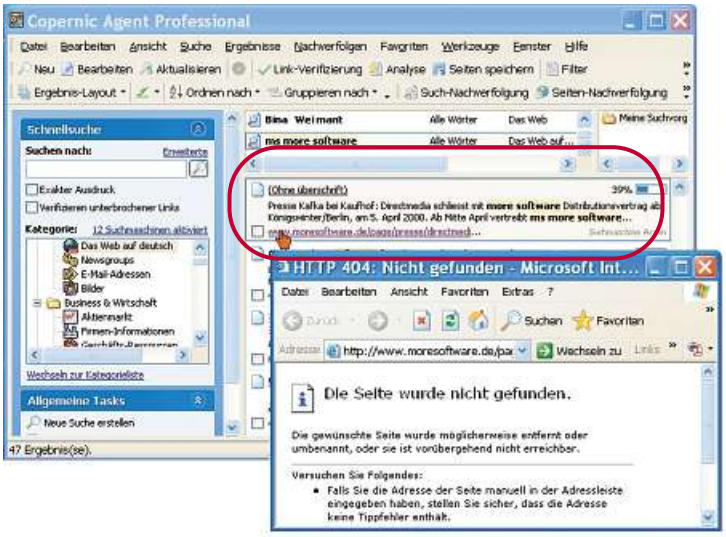
## Legal auf Spionagetour

Für den ersten Schritt einer Spionagetour im Web nutzt ein Internet-Detektiv Metasuchtools, die mehrere Suchmaschinen abfragen und die Resultate einem eigenständigen Ranking unterwerfen. So gleicht er die Schwächen einzelner Search-Engines aus, deren Betreiber bestimmte Webseiten nach moralischen oder politischen Gesichtspunkten herausfiltern. Typische Metasuchprogramme sind beispielsweise Copernic Agent *(www.copernic.com)* und Webferret *(www.webferret.com)* für den PC und die Adresse *www.dogpile.com* als Web-gestütztes System.

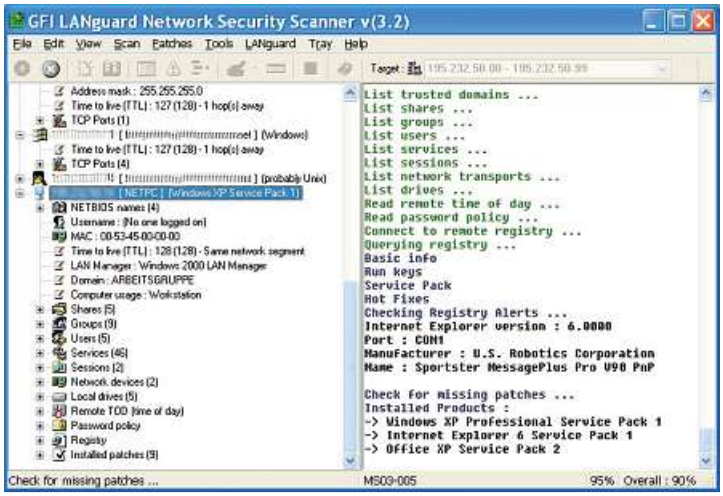
Möchte der Social Engineer einen Mitarbeiter eines Unternehmens ausfindig machen, der ihm Zugang zu geheimen Daten verschaffen kann, gibt er etwa die Web-Adresse des Unternehmens und einen Begriff wie »Lebenslauf« oder eine Berufsbezeichnung als Suchwörter ein. Auf diese Weise findet er private Websites von Mitarbeitern, die zu ihrem Arbeitgeber verlinkt haben und zugleich persönliche Lebensdetails sorglos verraten. *PC Professionell* entdeckt bei Tests für diesen Artikel den Angestellten eines deutschen Elektrokonzerns, der sogar seine Lieblingskneipe verrät: ein perfekter Ansatzpunkt für einen Übergang zum direkten Kontakt, zumal auch ein Bild nicht fehlt. Der Anwender sollte sich daher bewusst machen, welche Informationen über ihn frei zugänglich sind, um Kenner dieser Daten nicht automatisch als vertrauenswürdig einzustufen.

Über die Whois-Funktion auf *www.networksolutions.com*, *www.denic.de* oder *www.ripe.net* lässt sich die Adresse des Website-Besitzers herausfinden und damit – über Stadtplan und Satellitenbildprogramme – das Wohnumfeld analysieren. Whois liefert auch Domain-Server-Daten. Mit den Betriebssystem-Programmen Traceroute oder Tracert kann ein Angreifer dann Details über den Verbindungsweg zum Opfer erkennen, zum Beispiel die Server- und Router-Struktur bei dessen Provider. Diese Systeme können interessante Logfiles enthalten. Der Besitzer einer eigenen Website kann einiges dafür tun, Informationen zumindest nicht ungewollt über Dokumente preiszugeben. Er sollte den HTML-Quellcode auf verräterische Kommentare hin prüfen, bevor er ihn freigibt. Dateien von Office-Paketen enthalten oft Angaben über den Autor, seinen PC, eventuell seinen Arbeitgeber und über Personen, die die Dokumente weiter bearbeitet haben. Diese Informationen lassen sich zum Teil in den Dialogfeldern der *Eigenschaften*-Funktion entfernen. Darüber hinaus bleiben in Microsoft-Office-Dateien häufig Bruchstücke gelöschter Passagen und Hinweise auf den Speicherort der Dateien zurück. Vor allem wenn die Schnellspeicherung eingeschaltet ist. Ein Hexeditor macht diese Fragmente sichtbar. Der Wechsel zum PDF- oder TXT-Format schützt vor diesen verräterischen Infos.

Ein beliebter Trick der Social Engineers besteht darin, das Usenet über *www.google.com* nach den typischen Endungen von Unternehmens-E-Mail-Adressen zu durchsuchen. Im Test fand sich innerhalb weniger Sekunden ein Mitarbeiter eines großen US-Autokonzerns, der sich an einer Diskussion über Pädophilie beteiligte und damit Angriffspunkte bot. Administratoren laden zu einem Hack-Versuch geradezu ein, wenn sie im Online-Dialog Sicherheitsprobleme ihres Netzwerks preisgeben und dabei die E-Mail-Adresse ihrer Firma benutzen.




**▲ Nicht einmal Löschen hilft: Hier hat die Suchmaschine Acoon dem Copernic Agent Textbruchstücke aus einer Site geliefert, die längst nicht mehr existiert.**




▶ **Languard im Einsatz: Neben offen Shares bietet das Tool auch viele Infos über PCs an bestimmten IP-Adressen.**

## Die Tools und Tricks der Profispione

Die Grenze zwischen legaler und illegaler Informationsbeschaffung beschreibt beim Computer Based Social Engineering in der Regel §202a des Strafgesetzbuchs. Dieser legt fest, wann es jemandem erlaubt ist, fremde Daten einzusehen. Dabei gilt: Schutzmechanismen wie Kennwörter signalisieren Bereiche, die für ungebetene Gäste tabu sind. In offenen Verzeichnissen und auf Servern ohne Zugriffsrestriktionen darf ein Besucher Informationen ansehen, aber nicht manipulieren oder zerstören. Konkret bedeutet dies zum Beispiel, dass sich ein Webnutzer auf Einzelrechnern, die ein Tool wie Languard *(www.gfisoftware.de)* mit offenen, ungesicherten Shares im Internet gefunden hat, durchaus umsehen darf. Es liegt in der Verantwortung des Computerbesitzers, seine Daten vor neugierigen Augen zu schützen. Der Grund für die Regelung liegt darin, dass öffentliche Dienste sonst nur schwer von geschlossenen zu unterscheiden wären.

## Rückgriff auf Hacker-Methoden

Professionelle Industriespione stellen Kosten-Nutzen-Analysen an und dringen im Zweifelsfall lieber mit Tricks wie Zeitarbeit oder Dienstleistungen in ein Unternehmen ein, als viel Geld für eine technisch aufwändige Hacking-Aktion zu verschwenden. Im Social-Engineering-Umfeld hat es das Opfer eher mit bodenständigen Hack-Versuchen zu tun, muss dafür aber mit anderen raffinierten Tricks rechnen. Mit diesen Spezialitäten und den Hacking-Methoden befassen sich die folgenden Seiten. Social Engineers betrachten einen klassischen Hack eines Servers, den das Opfer regelmäßig nutzt oder besucht, als kostengünstige Alternative zu gezielten Abhöraktionen. Auf dem Server können persönliche Daten liegen, aber auch die Logfiles sind interessant. Zwar dürften nach dem deutschen Datenschutzgesetz viele Informationen gar nicht routinemäßig festgehalten werden, aber die meisten Server-Software-Produkte stammen aus den USA und laufen auch hier mit den dortigen Standardeinstellungen. Das bedeutet meistens auch intensives Logging.

Die klassischen Server-Angriffe sind es auch, die immer wieder die Basis für die gefürchteten Identitätsdiebstähle abgeben. Die Social Engineers sammeln die Kreditkartendaten und Authentifizierungs-Informationen lieber en gros auf schlecht geschützten E-Commerce-Servern ein, als die entsprechenden Risiken für eine einzelne Person einzugehen. Die Server werden auch heute noch zumeist über bekannte Schwachstellen geknackt, zu denen der Administrator die Patches noch nicht aufgespielt hat.

Zum Aufspüren der Sicherheitslücken zweckentfremden Social Engineers Tools, die der Schwachstellenanalyse durch Administratoren im eigenen Netz dienen sollen. Beliebt ist zum Beispiel das Client-Server-Tool Nessus *(www.nessus.org)* aus der Open-Source-Szene. Es besteht aus einem Server-Modul, das unter Unix-Derivaten läuft und die eigentlichen Suchaktionen durchführt, und Clients, über die autorisierte Anwender die Scans starten können. Nessus arbeitet mit einer immer wieder aktualisierten Liste bekannter Sicherheitslücken. Eine Eigenschaft des Tools ist, dass es laufende Dienste auch an ungewöhnlichen Ports findet. Versteckt ein Administrator einen Webserver zum Beispiel auf TCP-Port 8888, wird dieser Server bei einer Nessus-Attacke trotzdem mit einem CGI-Angriff auf Schwachstellen abgeklopft. Als Portscanner, der offene Zugangsmög-

lichkeiten zu einem System findet, benutzen Angreifer gern Nmap *(www.insecure.org)*. Das Tool sucht nach UDP-Ports, TCP-Ports oder einfach nach aktiven Host-Rechnern. Anwender, die Sicherungssysteme installiert haben, müssen wissen, dass Nmap seine Scans verstecken kann. Ein Trick besteht darin, zur Prüfung eines Ports ein FIN-Paket (Final Flag) zu schicken, das normalerweise eine Verbindung schließt. Offene Ports ignorieren dies als offensichtlichen Fehler, da ja keine Verbindung aktiv war. Ein geschlossener Port aber sendet trotzdem ein RST-Paket (Reset Flag), um die Scheinverbindung abzubrechen. Firewalls ignorieren diesen unverständlichen Datenverkehr häufig und melden deshalb keinen Portscan.

## Tückische E-Mail-Tricks

Social Engineers nutzen zudem E-Mails unter falscher Flagge. Die Absenderadressen lassen sich durch geschickte Server-Konfigurationen oder Telnet-Angriffe manipulieren. Anwender müssen vor allem mit Lock-E-Mails auf gefälschte Websites rechnen. So könnte sich ein Social Engineer als Support-Mitarbeiter eines Providers ausgeben und seine Zielperson auf eine Seite locken, auf der sie Zugangs- oder Abrechnungsdaten eingeben muss. Diese Seite ist dann in der Regel den Seiten des tatsächlichen Geschäftspartners der Zielperson nachgestaltet, liegt aber auf einem anderen Server.

Ein Grund, warum dieser Trick immer wieder funktioniert, ist die Unübersichtlichkeit und Länge typischer personalisierter Links, mit denen auch legitime Transaktionen abgewickelt werden. Kaum jemandem fällt auf, wenn der Server am Anfang etwa *www.ihrprovider.de.ru* oder *www.ihrporvider.de* statt *www.ihrprovider.de* heißt oder die Zeichenkette am Ende obskure Anweisungen enthält. Letzteres kann der Fall sein, wenn der Angreifer einen eigenen Frame in eine ansonsten unangetastete Seite geschmuggelt hat, etwa mit einer angeblichen Kundenumfrage einer Bank samt Bestätigung mit PIN und TAN. Genau so gut kann er eine gefälschte Mitteilung im Firmen-Intranet ablegen und Passwörter abfragen.

Wer befürchtet, eine gefälschte E-Mail erhalten zu haben, sollte sich den Mail-Header ansehen (siehe Beitrag »Falsche Fährten« auf Seite **2005**).

User machen Social Engineers geradezu ein Geschenk, wenn sie auf ihren Rechnern Verzeichnisse freigeben und sich dann mit dem Internet verbinden. Fürs interne Netz geöffnete Shares können nämlich auch aus dem Internet heraus gelesen werden. Dem Angreifer hilft dabei der Netzwerk-Scanner Languard, der entsprechende Rechner und Verzeichnisse ausfindig macht. Bei PCs, die per Dial-up-Verbindung online sind, ist ein gezielter Spionageversuch schwierig. Anders sieht es aus, wenn der Angreifer gezielt eine feste IP-Range durchsucht. Hier besteht die Möglichkeit, Informationen zu geheimen Projekten zu finden oder ein geeignetes Opfer zu identifizieren. Letzteres ist für einen Social Engineer viel wichtiger.

## Dem Opfer immer näher

Bei ernsthaften Social-Engineering-Angriffen, die hohen Gewinn versprechen, ist es denkbar, dass sich der Angreifer Zutritt zum PC des Opfers im Unternehmen verschafft. Erreicht er sein Ziel, könnte er Spionage-Software direkt installieren oder, wenn der PC mit starken Passwörtern oder weiteren Authentifizierungsmechanismen gut geschützt ist, einen so genannten Hardware-Keylogger einschleifen. Ist der PC ungeschützt, ist auch eine schnelle Sicherheitskopie aller Daten denkbar. Der technischen Suche nach Informationen folgt beim Social Engineering schließlich die Auswertung im direkten Kontakt mit dem Opfer oder Personen, die das Opfer kennen. Der Social Engineer hat nun genug Material zusammen, um das Vertrauen der Person zu gewinnen – hat er doch angeblich mit den gleichen beruflichen Widrigkeiten zu kämpfen. Oder er übertölpelt die Sekretärin der Personalabteilung, weil er nach der »K-Akte für Bremen Außen für Dr. Meier aus B 17« fragt und nicht nach diffusen Außendienstinformationen. Das Ziel ist erreicht: Die Mitarbeiter werden ihm bereitwillig helfen. HME




**▲ Social Engineering für alle: In den USA kann man Tools für dubiose Hintergrundrecherchen übers Web erwerben.**

# Die nächste Stufe

**Entscheidende Verbesserungen in puncto Sicherheit und einen Schutz vor Datenmissbrauch soll der Windows-XP-Nachfolger Longhorn integrieren.**

Eric Tierling, Heiko Mergard

Für Anwender, die Systemsicherheit und Stabilität an die erste Stelle setzen, soll Longhorn einen großen Fortschritt bringen: Das Betriebssystem wird mit zusätzlichen ausgefeilten Schutzfunktionen aufwarten. Einige davon machen sich schon beim Start bemerkbar. Der Anmeldedialog wurde überarbeitet. So ist der Austausch gegen ein anderes Winlogon-Modul nicht mehr möglich.

Der Internet Explorer beinhaltet nun auch einen Pop-up-Blocker, um das Erscheinen von Werbefenstern beim Surfen zu verhindern. So sollen auch Schädlinge ausgesperrt werden, die sich auf diesem Wege insbesondere unerfahrene Anwender als Opfer aussuchen und diese mit vermeintlich vielversprechenden Klick-Aufforderungen ködern.

Serienmäßig wird der Windows-XP-Nachfolger Komponenten zur Nutzung der neuesten Version 2 des Microsoft-Rechteverwaltungssystems (Rights Management Services, RMS) enthalten. RMS soll unter anderem einen Unternehmens-übergreifenden Schutz bieten und sich leichter bedienen lassen.

## Neues Identity System

Die elektronische Kommunikation mit anderen Personen und Unternehmen im Netz soll vor allem über eindeutige digitale Identitäten sicherer werden. Das zugehörige Identity System von Longhorn zeichnet für die Erkennung von Identitäten verantwortlich sowie die entsprechende Verwaltung der auf dem eigenen Computer befindlichen iCards (Information Cards). Gleichzeitig merkt sich das System, an wen die eigene iCard bislang bereits übertragen wurde. Das erleichtert spätere Aktualisierungen von Informationen beispielsweise nach einem Umzug.

Grundlegend betrachtet Longhorn alle Kontakte als Identitäten. Diese werden als Objekte direkt im WinFS-Dateisystem gespeichert und mit zahlreichen Informationen verknüpft. Hierzu gehören beispielsweise die E-Mail-Adresse und weitere Angaben, die der Benutzer zur Veröffentlichung freigegeben hat wie beispielsweise seine Postanschrift. Auch sein Public-Key-Zertifikat, das entweder vom lokalen System oder einer Active-Directory-Zertifizierungsstelle ausgestellt wird, falls der Benutzer einer Domäne angehört, bleibt in einem solchen Objekt gespeichert. Zusammen mit Verwendungsrichtlinien, die festlegen, dass zum Beispiel Telefon- und Handy-Nummern nicht an Dritte weiterzugeben sind, werden diese Informationen von Longhorn entsprechend als iCard gespeichert und im Kontakt-Explorer angezeigt.




▲ **Die Winlogon-Komponente wird für Longhorn überarbeitet. Der Austausch gegen ein alternatives Winlogon ist nicht mehr möglich.**

## iCards, Firewall und Freigaben

Zertifikate und iCards dienen bei Longhorn dazu, die Kommunikation in Intranet und Internet deutlich sicherer zu gestalten. Auf der PDC-Konferenz in Los Angeles erhielt *PC Professionell* erste Einblicke in das Longhorn-Identity-System und dessen praktische Anwendung. So greift in einem Fallbeispiel die Internet-Verbindungs-Firewall (ICF) auf iCards zurück, um Remote-Benutzern den Zugriff auf freigegebene Ordner des PCs zu gewähren: Nachdem der externe Nutzer seine iCard übermittelt hat und somit seine Iden-

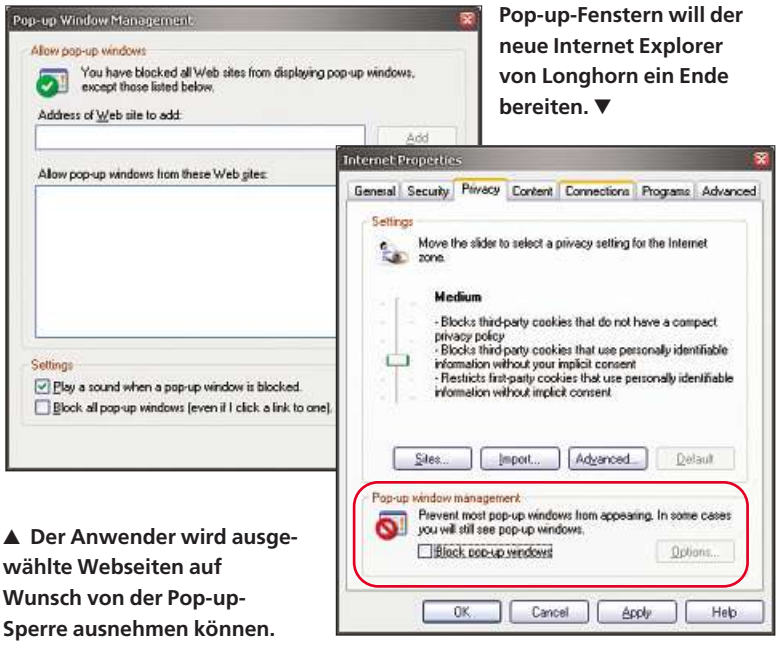
tität sichergestellt ist, kann für ihn eine Berechtigung zur Remote-Nutzung eines freigegebenen Ordners erstellt werden. Erst wenn diese Bedingungen – iCard-Prüfung, Ordner-Freigabe, Berechtigung – erfüllt sind, kann ein Fernzugriff auf den freigegebenen Ordner über das Netzwerk erfolgen. Andernfalls wird selbst ein Ping auf den Ziel-Computer, auf dem sich die Freigabe befindet, von der Longhorn-ICF abgewiesen. Entweder kennt das System die benötigte iCard nicht oder es existiert für diesen Benutzer noch keine Freigabe-Berechtigung. Auf diese Weise verfügt Longhorn neben Authentifizierung und Authorisierung über eine zusätzliche Schutzebene. Diese reduziert die Angriffsfläche des Computers einfach aber wirkungsvoll.

Weitere Einsatzgebiete für das neue Identity System umfassen zum Beispiel sichere E-Commerce-Anwendungen. Nach der Übertragung der iCard an den Anbieter ist dieser in der Lage, den Benutzer künftig zuverlässig zu identifizieren. Das soll etwa Bestellungen und Zugriffe auf geschützte Dokumente vereinfachen. Genauso ist es Microsoft zufolge denkbar, dass der Benutzer Anbietern die Berechtigung einräumt, Einträge wie etwa Liefertermine im Kalender des lokalen PC vorzunehmen oder – im Falle Microsofts – selbstständig Patches einzurichten. Ob die Anwender genügend Vertrauen in dieses Verfahren setzen oder stattdessen lieber auf diese Automatisierungsfunktion verzichten, bleibt abzuwarten.

## Sicherheit für Unternehmen

Anders als beim Passport-Verfahren, dem ersten Identitätsverwaltungs-Ansatz von Microsoft, soll das Longhorn-Identity-System auch die Kommunikation zwischen Unternehmen absichern. Beispiel: Das Unternehmen A übermittelt seine iCard an das Unternehmen B. Nach erfolgreicher Identitätsprüfung im Active Directory des Unternehmens B wird ein Organisationsobjekt für das Unternehmen A erstellt. Wenn ein Benutzer aus dem Unternehmen A mit dem Unternehmen B Kontakt aufnimmt, wird dieser als vertrauenswürdig erkannt. So genannte Trustbridges, die den Schlüssel der iCard des Organisationsobjekts verwenden, erlauben es dabei, die Identität des fremden Benutzers zu verifizieren. Der passende Trustbridge-Server wird voraussichtlich mit Erscheinen der Longhorn-Server-Ausführung auf den Markt kommen oder darin bereits enthalten sein.

In ganz ähnlicher Weise nutzt Indigo, das Kommunikations-Subsystem von Longhorn,




**Pop-up-Fenstern will der neue Internet Explorer von Longhorn ein Ende bereiten. ▼**

**▲ Der Anwender wird ausgewählte Webseiten auf Wunsch von der Pop-up-Sperre ausnehmen können.**

die Trustbridges. Damit schafft Indigo für Web-Applikationen sichere Verbindungen. Hier arbeitet Indigo mit WS-Security zusammen, dem Sicherheitsprotokoll für Webdienste. Auf längere Sicht dürfte der Anwender somit den Vorteil haben, sich bei der Nutzung unterschiedlicher Webdienste nur einmal anmelden zu müssen (Single-Sign-on).

## Programme sicher ausführen – mit und ohne Admin-Berechtigung

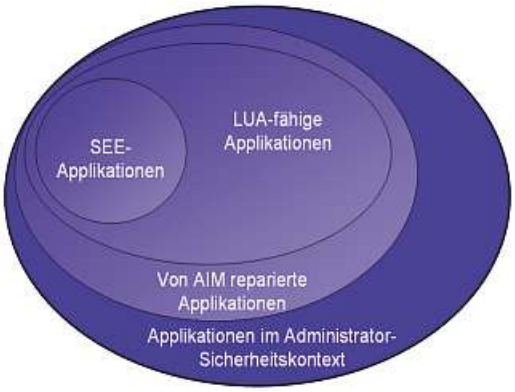
Ein weiteres Feld, in dem Longhorn Neuerungen bietet, betrifft die geschützte Ausführung von Programmen. Die neue Code Access Security (CAS) soll es ermöglichen, dass selbst ein als Administrator angemeldeter und mit weitreichenden Berechtigungen versehener Benutzer Applikationen wie etwa einen Webbrowser mit weniger Privilegien ausführt. Dieses Protected Admin genannte Prinzip macht sich auch das Secure Execution Environment (SEE) zunutze, das vereinfacht ausgedrückt auf standardmäßig gewährten CAS-Berechtigungen beruht. Destruktiver Code hat es somit wesentlich schwerer, sich in das System einzuschleichen und Schaden anzurichten oder Informationen aus Festplattenordnern auszuspionieren.

SEE ist insbesondere für Web-Szenarien und unerfahrenere Benutzer konzipiert, da keine Entscheidungen zu treffen sind. Die Technologie lässt sich aber genauso für lokale Anwendungen heranziehen. CAS und SEE sind dabei immer den Berechtigungs-Limits des angemeldeten Benutzers unterworfen und




▲ **In den bei WinFS hinterlegten iCards speichert Longhorn die Identitäten von Benutzern mitsamt Kontaktdaten und Zertifikaten.**

können keine weitergehenden Privilegien konsumieren. Schon unter Windows 2000 hatte Microsoft das Konzept der sekundären Anmeldung (Secondary Logon) eingeführt. Damit startet der Anwender Programme im Sicherheitskontext eines anderen, typischerweise mit Administrator-Rechten ausgestatteten Benutzers, ohne den aktuellen Windows-Desktop per Abmeldung verlassen zu müssen. Für das normale Arbeiten reicht es somit aus, als einfacher Benutzer am System angemeldet zu sein, der nur wenige Privilegien besitzt – zumindest in der Theorie: Die Erfahrungen auch mit Windows XP zeigen allerdings, dass nur wenige Hersteller ihre Software so programmieren, dass diese den Systemstatus nicht verändern möchte und im Sicherheitskontext eines Benutzers mit limitierten Privilegien (Least-Privileged User Account, LUA) korrekt oder wie gewünscht läuft.




▲ **Mit einem mehrstufigen Security-Konzept sorgt Longhorn für die sichere Ausführung von Applikationen – sowohl im Administrator- als auch im Benutzer-Kontext.**

Vielmehr sind hier Fehler an der Tagesordnung. Das führt häufig dazu, dass der Benutzer sich lieber als Administrator anmeldet und somit Angreifern, Viren und Trojanern Tür und Tor öffnet.

## Sicherer Administrator-Trick

Für Longhorn gestaltet Microsoft es erheblich einfacher, sich als normaler Benutzer anzumelden und trotzdem mit Programmen zu arbeiten, die zur Ausführung eigentlich eine Administrator-Berechtigung benötigen. Diesen Trick soll eine Technologie namens Application Impact Management (AIM) vollbringen. AIM simuliert eine virtuelle Administrator-Umgebung für Applikationen, die im LUA-Sicherheitskontext ablaufen. Die Zugriffsberechtigungen der Anwendungen werden im laufenden Betrieb angepasst. Analog dazu können sich Administratoren als solche anmelden und zusätzlich zu Applikationen mit voller Berechtigung gleichzeitig auch solche Programme aufrufen, die lediglich in einem eingeschränkten Sicherheitskontext aktiv werden. Zudem überwacht AIM kritische Systemvorgänge und macht diese bei Bedarf wieder rückgängig. Auch die Installation der betreffenden Anwendung lässt sich rückgängig machen. Allerdings setzt AIM voraus, dass im LUA-Sicherheitskontext ablaufende Programme eine Beschreibungs-Datei mitbringen. Diese versorgt Longhorn mit den notwendigen Informationen und ist von offizieller Seite digital signiert. Ob die Software-Produzenten hier mitziehen oder wie lange es dauert, bis AIM genügend Unterstützung erfährt, muss sich allerdings erst noch erweisen.

## NGSCB als Basis für sicheres Computing

Auf der Hardware-Entwicklerkonferenz WinHEC demonstrierte Microsoft erstmals die Funktionsweise seiner ehemals unter dem Codenamen Palladium bekannten Next Generation Secure Computing Base (NGSCB). Jetzt nimmt dieses Sicherheits-Konzept immer konkretere Gestalt an. Prinzipiell teilt NGSCB das Betriebssystem in eine linke und eine rechte Seite, »LHS« (Left Hand Side) und »RHS« (Right Hand Side). Die linke Seite entspricht weitestgehend dem bekannten Standard-Modus des Windows-Betriebssystems. Darin laufen Anwendungen und Treiber genauso wie Viren, Trojaner und dergleichen parallel. Die Unterschiede gegenüber heutigen Systemen fallen überaus gering aus. So sind beispielsweise komplette Speicher-

transfers sowie das Umschalten des Prozessors in den Real-Modus nicht erlaubt.

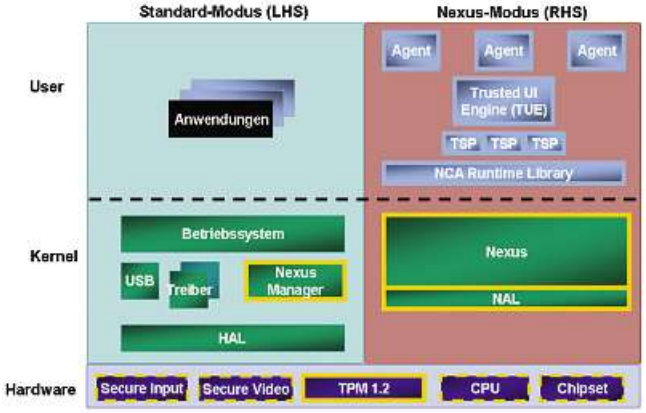
Mit der rechten Seite erwacht NGSCB jedoch zum Leben: Im Zentrum befindet sich der Nexus getaufte Security-Kernel. Diese Betriebsart wird auch als Nexus-Modus bezeichnet. Bei dieser Sandbox-Umgebung steht Sicherheit an erster Stelle. Deshalb findet die Anbindung von Hardware-Komponenten über einen eigenen Abstraktions-Layer, den Nexus Abstraction Layer (NAL), mit eigenen Treibern statt. Ferner benötigt Nexus zwingend einen an die Hauptplatine gebundenen Chip, sodass die Verwendung von NGSCB Änderungen an der Hardware erfordert. Unter Umständen müssen Benutzer neue PCs kaufen, die die entsprechenden Anforderungen erfüllen. Von NGSCB gesicherte Anwendungen stellen dann Agenten dar, die ihrerseits in geschützten Bereichen des Arbeitsspeichers ablaufen. Das soll zusammen mit der Hardware-Bindung Manipulationen an Code, Speicherinhalten oder übertragenen Paketen zuverlässig verhindern.

Während das Motto für LHS Kompatibilität zu existierender Software lautet, fällt der RHS die Aufgabe zu, für erhöhte Sicherheit zu sorgen. Grundsätzlich misstraut der Nexus-Modus der LHS und tauscht daher mit dieser Seite Daten nur über den eigens dort implementierten Nexus Manager aus. Prüfungen tragen dazu bei, dass auf diesem Wege keine fehlerhaften oder ungültigen Informationen zur RHS gelangen.

Die Verfechter von NGSCB, allen voran die in der Trusted Computing Group (ehemals Trusted Computing Platform Alliance, TCPA) zusammengeschlossenen Hersteller, versprechen, dass ihr Security-Verfahren für mehr Sicherheit beim Umgang mit Daten sorgen werde. So hätten beispielsweise Trojaner keine Chance mehr, Informationen einer Online-Banking-Applikation aus dem Arbeitsspeicher auszulesen und missbräuchlich zu verwenden. Kritiker hingegen sehen in NGSCB eine Technologie, die in erster Linie den Interessen der Software- und Medien-Industrie dient. Dementsprechend ermöglicht die Technologie wie nie zuvor, Urheberrechts- und Kopierschutzregelungen auf allen PCs durchzusetzen.

## Aktueller Stand

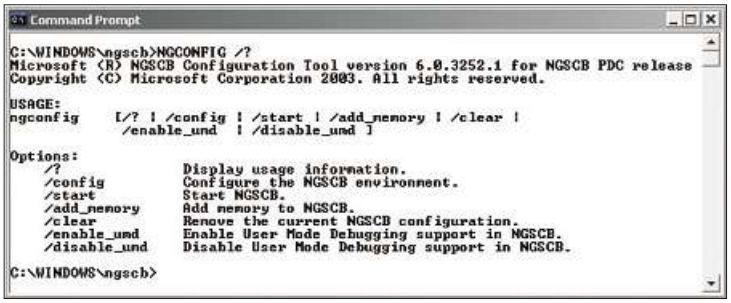
Rein technisch betrachtet ist Longhorn von all dem aber noch weit entfernt. Die PDC-Build 4051 installiert zwar den versteckten Ordner namens NGSCB, doch dieser weist lediglich wenige Dateien und Unterordner auf. Zudem




**▲ Die Sicherheits-Technologie Next-Generation Secure Computing Base (NGSCB) setzt spezielle Hardware voraus. Das System wird unterteilt in einen hochkompatiblen Standard- sowie einen sicheren Nexus-Bereich.**

muss der Anwender den Nexus-Modus derzeit noch mit dem Befehlszeilen-Programm *ngconfig* von Hand aktivieren. Da eine automatische Speicherverwaltung noch nicht existiert, ist die Größe des vom RHS verwendbaren Arbeitsspeichers ebenfalls manuell zu deklarieren. Zurzeit ist NGSCB also höchstens rudimentär implementiert. Bis zum Marktstart von Longhorn soll allerdings die erste Version dieser Sicherheits-Technologie fertig gestellt und im Lieferumfang des Betriebssystems enthalten sein.

Selbst, wenn Longhorn noch Zukunftsmusik darstellt, ist schon jetzt klar: Die kommende Windows-Version wird mit einer Reihe von neuen, besseren Sicherheitsmerkmalen versehen sein, von denen Anwender unmittelbar profitieren. Von vielen Funktionen liefert die Longhorn-Build 4051 aber noch keinen oder nur einen schwachen Vorgeschmack. Viele Features stecken noch genauso in der Entwicklungsphase wie das Betriebssystem selbst. HME




**▲ Bei der vorliegenden Entwickler-Version von Lonhorn muss die Nexus-Konfiguration ebenso manuell erfolgen wie das Starten und Beenden dieser sicheren Umgebung.**

# Drahtlos unsicher

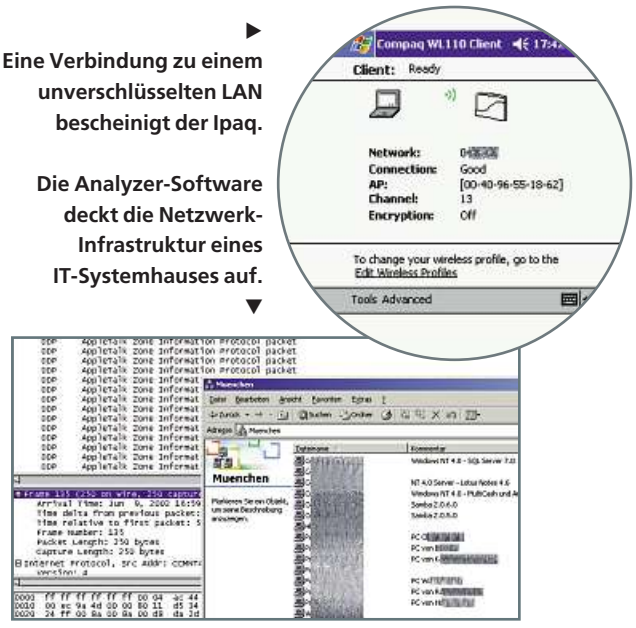
**Mit vergleichsweise wenig Aufwand spüren Hacker ungeschützte Wireless-LANs auf, dringen unbemerkt in Netzwerke ein und stehlen sensible Daten.**

Stefan Greiner

Ursache für die meisten erfolgreichen Einbrüche in drahtlose Netzwerke sind die Werkseinstellungen von WLAN-Routern und Access-Points. Um eine schnelle Plug-and-Play-Erstinstallation zu erleichtern, verzichten viele Hersteller auf das standardmäßige Setzen der Sicherheitseinstellungen und überlassen das dem Käufer selbst. Hat dieser das Handbuch nicht gründlich studiert oder die Installation nach der ersten Verbindung beendet, wird Besuchern Tür und Tor geöffnet.

## Offene WLANs an allen Orten

Zudem ermöglichen viele WLAN-Systeme ein komfortables Ad-hoc-Networking. Dabei läuft die Identifizierung, Authentifizierung und Anmeldung (Autorisierung) der Clients automatisch ab. Zwar sehen WLAN-Systeme Sicherheitsmechanismen vor, durch die zum Teil erheblichen Lücken bei deren Umsetzung sind Angriffe aber relativ leicht möglich.




▶ **Eine Verbindung zu einem unverschlüsselten LAN bescheinigt der Ipaq.**

**Die Analyzer-Software deckt die Netzwerk-Infrastruktur eines IT-Systemhauses auf.** ▼

Ein Einbruch in ein ungeschütztes WLAN stellt für Hacker also keine große Hürde dar. Da sich elektromagnetische Wellen in alle Richtungen ausbreiten, ist ein Abhören oder Senden möglich, ohne dass beispielsweise in das Gebäude eingedrungen werden muss. Gegenüber herkömmlichen festverdrahteten LANs ist bei einem WLAN jeder, der sich im Empfangsbereich befindet, ein potenzieller Teilnehmer des Netzwerks. Selbst Anwender ohne böse Absichten können ungeschützte WLANs aufspüren. Nicht selten wird einem Anwender bei der Einrichtung seines eigenen Wireless-Netzwerk auch die Verbindung zu einem anderen WLAN angeboten. Das ist in Bürogebäuden, Studentenwohnheimen oder größeren Wohnsiedlungen nicht ungewöhnlich. Je nach Ausstattung, Technik und Konfiguration bieten Access-Points Reichweiten von unter 20 bis zu rund 450 Meter mit entsprechenden Verstärkern.

## Mit wenig Aufwand zum Ziel

Meist reicht Hackern ein Notebook mit Wireless-Karte aus, die er dort in Betrieb nimmt, wo er WLANs vermutet. Mit einem Tool wie NetStumbler *(www.netstumbler.com)* scannt der Hacker nacheinander alle Funkkanäle ab und bekommt im Idealfall eine Verbindung.

Bekannt sind auch Fälle, bei denen sich Angreifer, so genannte Wardriver, mit Notebook und Dachantenne durch Innenstädte chauffieren ließen und innerhalb weniger Minuten zahlreiche offene Netzwerke orten konnten. Dabei handelt es sich nicht nur um private WLAN-Installationen, sondern auch um Firmennetze, bei denen man solch Sicherheitslücken nicht vermuten würde. Unauffälliger als mit dem Notebook arbeitet sich mit einem Pocket-PCs. Den Wardrivern geht es nicht darum, Daten in den Netzwerken von Privatleuten oder Firmen zu stehlen oder diese zu zerstören. Sie möchten über offene WLANs kostenlos ins Internet gelangen. Dass sich

Wardriver in einer rechtlichen Grauzone bewegen, wissen sie sehr wohl. In den seltensten Fällen werden die Betreiber ungesicherter WLANs über die Sicherheitslücken ihrer Netze informiert. Zu hoch ist die Angst vor rechtlichen Konsequenzen.

Das erfolgreiche Wardriving ist nur deshalb möglich, weil viele WLANs unzureichend geschützt sind. Die Betreiber nutzen keine der möglichen Sicherungsmethoden, wie beispielsweise WEP-Verschlüsselung oder MAC-Filtering, bei dem festgelegt wird, mit welchen Netzwerkkarten ein Access-Point überhaupt kommunizieren darf und mit welchen nicht.

Auf diversen Internet-Seiten und in Foren werden die Standorte erfolgreich georteter offener Wireless-LANs veröffentlicht. Interessierte können sich somit mühelos in solche Netze einklinken, ohne selbst suchen zu müssen. Sogar Luftaufnahmen oder Straßenpläne mit exakter Position sind verfügbar. Eine andere Möglichkeit WLANs mit freiem Zugang zu kennzeichnen, ist das Aufmalen von Kreidezeichen auf der Straße oder an der Gebäudefront, das Warchalking. Was für Unwissende wie ein kryptisches Gebilde aussieht, ist eine Information der Wardriver, die damit auf offene WLAN-Spots hinweisen.



◀ **Mit Wireless-LAN-Karte, Notebook, Ipaq und Zusatzantenne ist das Ausspähen ungesicherter Funk-Netzwerke aus dem Auto heraus kein Problem.**

## Schutzmaßnahmen

Der elementarste Schutz ist der des Access Points (AP). Alle Sicherheitsmaßnahmen helfen nichts, wenn ein Eindringling den AP nach Gutdünken umkonfigurieren kann. Auf jeden Fall muss daher das Passwort der Basisstation unmittelbar nach Inbetriebnahme geändert werden – die Default-Einstellungen gängiger Hersteller sind Hackern meist bekannt und können so leicht umgangen werden. Sinnvoll ist es außerdem, auch die IP-Adresse zu ändern, unter der ein Access Point angesprochen werden kann. Der Administrator sollte einen anderen Adressbereich als den vom Hersteller vorgegebenen verwenden (zum Beispiel 192.168.137.x statt 192.168.1.x).

Sehr wichtig zum WLAN-Schutz ist die Datenverschlüsselung mit Wired Equivalent Privacy (WEP) auf der Funkstrecke. Ältere WLAN-Produkte arbeiten mit 40-Bit-Verschlüsselung, neuere zusätzlich mit 104 Bit langen Schlüsseln. Soll im Funknetz auch nur ein Endgerät mit der kürzeren Schlüssellänge eingebunden werden, müssen alle Geräte im 40-Bit-Modus arbeiten.

Einige Geräte erlauben auch, die volle Schlüssellänge von 64 oder 128 Bit mit einem komplett eigenen Code zu verwenden. Diese Schlüssel sind aber nicht mit WLAN-Komponenten kompatibel, die den 24-Bit-Header automatisch generieren. Ein Nachteil der Kodierung: Der Datendurchsatz sinkt.

Um den Schlüssel möglichst sicher zu machen, sollte der Anwender keinen Klartextschlüssel verwenden, sondern eine beliebige Buchstaben- und Zeichenkombination. Bei vielen WLAN-Karten muss der Schlüssel ohnehin als Hexadezimal-Sequenz eingegeben werden, so dass es keinen Unterschied im Bedienkomfort macht, ob der Schlüssel »Peter« oder »C9Z7k« lautet. MBA

## Handy-Spam via Bluetooth

Bekommen Anwender von Bluetooth-Handys an stark frequentierten Orten anonyme Mitteilungen aufs Display, könnten sie einem neuen Trend aufgesessen sein: Bluejacking ist zwar völlig harmlos, kann jedoch gehörig auf die Nerven gehen. Dabei wird die Möglichkeit, Kontakte an andere User zu senden, missbraucht: Der Bluejacker legt auf seinem Handy einen Kontakt an, füllt das Namensfeld jedoch mit einem Spruch seiner Wahl. Versucht er, den Eintrag per Bluetooth zu senden, listet das Gerät alle aktiven BT-Devices im Umkreis von zehn Metern auf. Das Auswählen des Opfers gleicht zwar einem Glücksspiel, doch genau dies verschafft Bluejackern den Kick. Angefunkte bekommen die Meldung auf ihr Display, ohne feststellen zu können, wer den Funk-Spam sendet. Webseiten wie *www.bluejackq.com* und *www.iblue jackedyou.com* beschäftigen sich nur damit, wo Bluejack-Opfer zu finden sind, und tauschen Erfahrungen aus. Bluejacking funktioniert auch an Orten ohne Mobilfunknetz, zudem ist der moderne Klingelstreich völlig kostenlos. Gegen den Spam hilft nur das Abschalten der Bluetooth-Funktion. Schlechte Aussichten also für Anwender, die per Bluetooth-Headset telefonieren und die Verbindung ständig aktiviert haben.




▲ **Bluejacking: Das Versenden anonymer Mitteilungen via Bluetooth nimmt immer mehr zu.**

# Security-Services

**Fehlt es kleineren Unternehmen an Erfahrungen im Bezug auf die Netzwerk-Sicherheit, empfiehlt sich der Einsatz von Managed Security-Services.**

Dirk Reichelt

Die hohe Zahl unterschiedlichster Sicherheitsanbieter macht es deutlich, welche Gefahren aus dem Internet drohen: Für das dritte Quartal 2003 meldet Internet Security Systems *(www.iss.net)* 725 neue Sicherheitsschwachstellen. 218 davon wurden als hohes Sicherheitsrisiko eingestuft. Message Labs *(www.messagelabs.com)* meldet für August 2003 über 16 Millionen gestoppte Mails, die mit dem Sobig-Virus infiziert waren. Neben Viren laden ungesicherte oder falsch konfigurierte Internet-Zugänge Hacker dazu ein, einen Angriff auf das dahinter liegende LAN zu starten. Die Folgen dieser verschiedenen Angriffe sind oft mehrstündige Ausfälle von Servern und Arbeitsplatzrechnern.

## Fehlendes Sicherheits-Know-how

In vielen kleinen Unternehmen fehlt es häufig an ausreichend Sicherheits-Know-how, um aus den Meldungen der verschiedenen Security-Systeme eine Gefahr für das eigene System zu erkennen und gezielte Gegenmaßnahmen einzuleiten. Während einige Dienstleister das komplette Spektrum an Sicherheitsleistungen abdecken, sind andere lediglich auf Teilaspekte spezialisiert. Bevor sich ein Unternehmen für einen MSS entscheidet, gilt es, den Bedarf im eigenen Unternehmen zu identifizieren. So kann das Outsourcing einzelner Teilbereiche des Sicherheitsmanagements den Rundumschutz des Netzwerks verbessern. Wer etwa über ein bewährtes Duo aus Firewall und IDS verfügt und zusätzlich eine Absicherung des Mail-Verkehrs sucht, findet bei Network Associates *(www.nai.com)* oder Message Labs sehr gute Angebote.

Wichtig für ein komplett sicheres Netzwerk ist, dass der gesamte ein- und ausgehende Verkehr überwacht wird. Hierfür müssen mindestens Sicherheitsdienste für Firewall, Mail und HTTP/FTP-Traffic vorhanden sein. Sollen zusätzlich Filialen oder verschiedene Betriebsteile sicher miteinander vernetzt werden, ist der Aufbau und das Management eines Virtual Private Networks (VPN) notwendig.




▲ **Web-Überwachung: Über eine sichere Webverbindung erfolgt das Fein-Tuning des Net-2580-Mail-Filters.**

## Das Funktionsprinzip von MSS

Mit dem Outsourcing des Sicherheitsmanagements wird die Kontrolle über den ausgelagerten Teilbereich direkt an den Dienstleister übergeben. Verschiedene Anbieter übernehmen dabei das komplette Management für bestehende Systeme und erweitern diese eventuell um eigene Software-Lösungen. Einige MMS erfordern die Installation zusätzlicher Hardware, auf der das System des MSS-Dienstleisters im eigenen LAN installiert wird. Über einen sicheren Kanal, wie etwa eine VPN-Verbindung, einen verschlüsselten SSH-Zugang oder eine ISDN-Einwahl kann der Dienstleister die Konfiguration verändern, Updates für den Virenscanner sowie andere Dienste einspielen und die Log-Daten für die Analyse abrufen.

Während die Kontrolle für HTTP-Downloads und andere Verbindungen aus dem

Netzwerk den Einsatz einer Firewall beim Übergang zwischen dem internen Netzwerk und dem Internet nötig macht, kann die Sicherheit des E-Mail-Datenverkehrs auf andere Art und Weise gewährleistet werden. Ein Eintrag im Domain-Name-Service (DNS) bestimmt, an welchen Server die Mails für eine bestimmte Domain zugestellt werden. Bei einer permanenten Verbindung mit dem Internet ist dies oft ein Mail-Relay, der in der DMZ der Firewall installiert wird.

Bei Dial-up-Zugängen mit dynamischen IP-Adressen werden Mails häufig beim Provider zwischengespeichert. Setzt man einen MSS für die E-Mail-Kontrolle nach Viren und Spam ein, kann der Eintrag für den Mail-Server im DNS geändert werden. Mails für die eigene Domain werden dann nicht mehr direkt an den eigenen Mail-Server zugestellt, sondern zuerst durch den Dienstleister überprüft. Erst nach dem Scan werden die Mails an den eigenen Mail-Server ausgeliefert. Mit der permanenten Analyse kann der MSS-Anbieter frühzeitig neuartige und bisher unbekannte Viren erkennen und diese zentral stoppen.

## Rundum sicher

Die komplette Sicherheit des LANs basiert auf der Aktualität von Virenscanner, Firewall-Regeln und System-Updates. Bei der Entscheidung für einen MSS sollten Firmen darauf achten, dass der Dienstleister eine permanente Überwachung anbietet. Häufig finden Angriffe aus Übersee über Nacht statt. Große MSS-Anbieter arbeiten mit weltweit verteilten Rechenzentren, die Angriffe jederzeit erkennen können und bei einer unmittelbaren Gefahr für die überwachten Systeme geeignete Gegenmaßnahmen ergreifen. Wichtig für den erfolgreichen Einsatz eines MSS ist, dass das komplette Sicherheitsmanagement mit dem Partner abgestimmt wird.

Setzt das Unternehmen etwa eine MSS für die Absicherung des E-Mail-Verkehrs ein, sollten Firewall-Policys und Content-Filterregeln dafür sorgen, dass der Zugriff auf private Mails per Web-Interface oder POP3 unterbunden wird. Wer eine Managed Firewall einsetzt, muss darauf achten, dass neben der Firewall keine andere Internet-Verbindung für das Netzwerk möglich ist.

## Normgerechte Systeme

Ein zielgerichtetes und standardisiertes Vorgehen beim Entwurf, bei der Einführung und bei der Nutzung von MSS ist mit ausschlaggebend für den späteren Erfolg des Sicherheitsmanagements. Mit der ISO-17799-Norm und der international anerkannten BS-7799-2b-Norm werden sinnvolle Vorgehensweisen für das Management der IT-Sicherheit vorgeschlagen. Auf Basis dieser Standards können Dienstleister ihre verwendeten Vorgehensmodelle und Verfahrensschritte für die Analyse, Einführung und Überwachung des Sicherheitsmanagements zertifizieren lassen.

## Nachteile von Managed Security-Services in der Praxis

Wie bei jedem anderen Outsourcing-Angebot auch ist die Entscheidung für einen Managed Security-Services mit Risiken verbunden. Durch die Nutzung eines MSS bekommt der Dienstleister Zugriff auf wichtige Systeme im Unternehmen. Mitunter werden vertrauliche Daten, zum Beispiel Mails, direkt über die Server des Dienstleisters geleitet. Gleichzeitig macht der Einsatz eines MSS die Öffnung eines Zugangs für die Fernadministration notwendig. Hierbei sollte man darauf achten, dass nur sichere Verbindungen wie etwa ein SSH-Zugang gestattet sind. Anderenfalls eröffnet ein solcher Zugang einem Hacker ungewollt einen neuen Angriffspunkt.

Mit der Entscheidung für einen MSS verliert das Unternehmen selbst ein Stück der Kontrolle über das eigene Sicherheitsmanagement. Um die Funktionsfähigkeit des Dienstes und einen umfassenden Schutz zu garantieren, bietet der MSS-Dienstleister häufig nur begrenzte Eingriffsmöglichkeiten in die Verwaltung des Sicherheitsdienstes. Hier ist es wichtig, schon vorab festzulegen, inwieweit der Sicherheitsbeauftragte der Firma später selbst die Möglichkeit zur Anpassung der Sicherheitseinstellungen hat. MBA

## Die häufigsten Attacken

| | | |
|---|---|---|
| 1 | Port 80 (Web/HTTP) | 45,5 Prozent |
| 2 | Port 137 (Netbios) | 20,2 Prozent |
| 3 | Port 1434 (SQL) | 13,7 Prozent |
| 4 | Port 1985 (HSRP) | 3,5 Prozent |
| 5 | Port 138 (Netbios) | 3,4 Prozent |
| 6 | Port 161 (SNMP in) | 3,3 Prozent |
| 7 | Port 162 (SNMP Trap) | 3,3 Prozent |
| 8 | Port 21 (FTP) | 1,8 Prozent |
| 9 | Port 443 (HTTPS) | 1,6 Prozent |

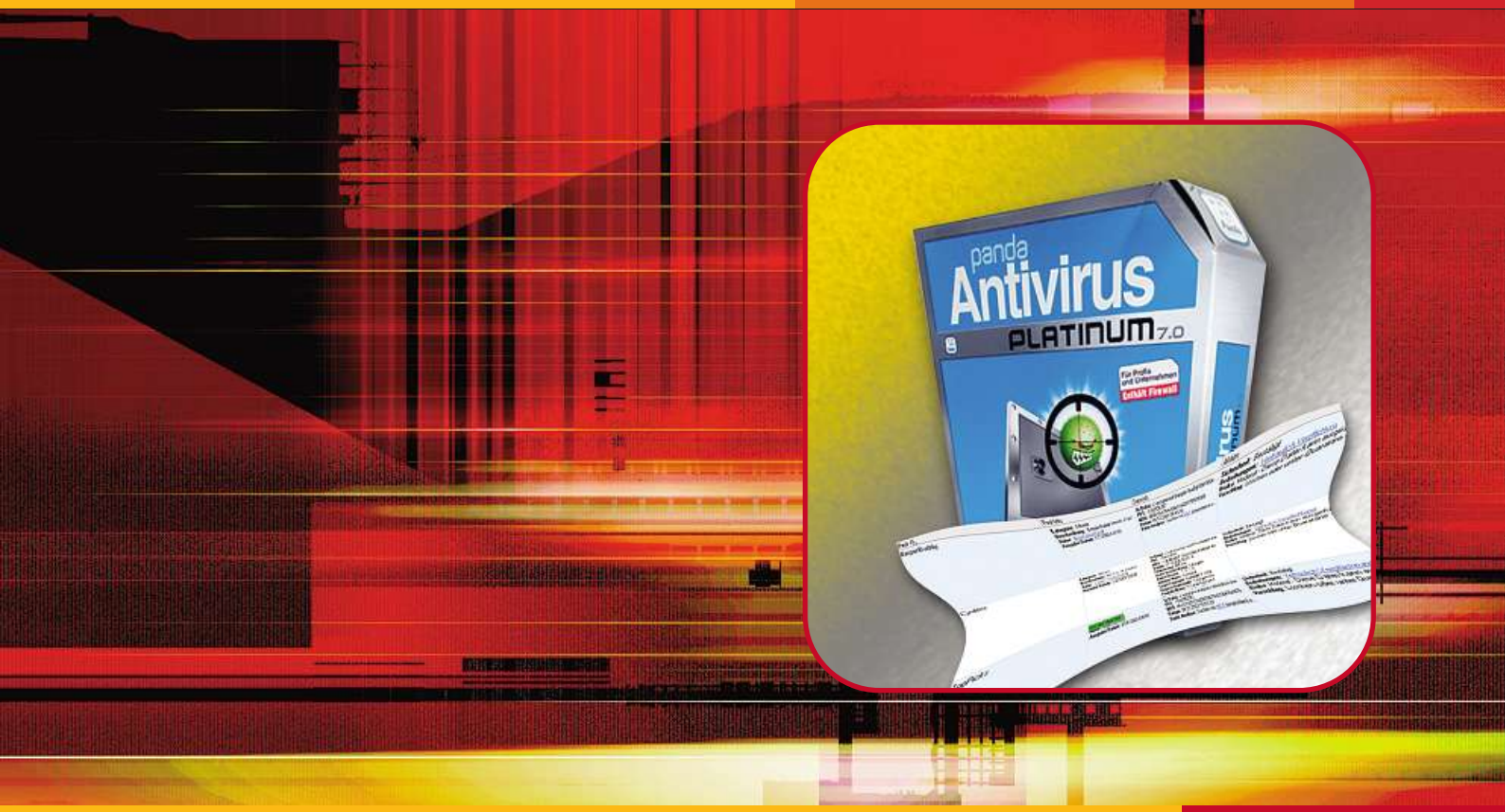
**Angriffsfläche:** Auf dem Port 80 werden immer noch die meisten Angriffe registriert. Der hohe Wert bei SQL ist den Slammer-Wurm zuzuschreiben.

# Managed Security-Services im Überblick

| Anbieter | Dimension Data Germany | IBM Deutschland | Message Labs | Network Associates | Pallas | Schwarz Computer Systeme |
|---|---|---|---|---|---|---|
| Internet | www.de.didata.com | www.ibm.de/security | www.messagelabs.com | www.nai.com | www.pallas.de | www.schwarz.de |
| Preis | ab 1250 Euro/Monat | ab 2000 Euro/Monat | ab 975 Euro/Jahr (25 User) | ab 43 Euro/Monat | 259 Euro/Monat (10 Arbeitsplätze) | ab 33 Euro/Jahr (50 User) |
| ISO 17799/BS 7799-2 zertifiziert | ○ | ● | ● | ○ | ○ | ○ |
| Überwachungszeitraum | 24 x 7 x 365 | 24 x 7 x 365 | 24 x 7 x 365 | 24 x 7 x 365 | 24 x 7 | 24 x 7 x 365 |
| Unterstützung dynamischer IPs | ○ | ● | ● | ● | ● | ● |
| Installation zusätzlicher Hardware beim Kunden notwendig | ● (im Preis nicht enthalten) | ○ | ○ | ○ | ● VPN-Appliance oder Router (im Preis enthalten) | ● im Preis nicht enthalten |
| Sichere Verbindung zwischen Kunden- und Control-Center | VPN/V-Tunnel Kunden und Control-Center | VPN | ○ | k. A. | VPN oder Direktverbindung | SSH, SSL-verschlüsselt |
| **Managed Services** | | | | | | |
| Firewall | ● | ● | ○ | ● | ● | ○ |
| Intrusion-Detection | ● | ● | ○ | ○ | ● | ○ |
| E-Mail | Antivirus | Antivirus, Spam-Schutz, Content-Filter | Antivirus, Spam-Schutz, Anti-Porn, Content-Control | Spam-Schutz | Antivirus, Spam-Schutz | Antivirus, Spam-Schutz |
| HTTP/S + FTP | FTP-Gateway | Content-Filter, Antivirus | ○ | Antivirus | Content-Filter, Antivirus | Antivirus |

| Anbieter | Securebox IT-Solutions | Siemens I&S IT PS | Symantec | Systemberatung Axel Dunkel | Telco Tech | Tenovis |
|---|---|---|---|---|---|---|
| Internet | www.securebox.at | www.siemens.com/itsecurity | www.symantec.de | www.dunkel.de | www.managed-security.de | www.tenovis.com |
| Preis | ab 1999 Euro (inklusive Service und Virenlizenz für ein Jahr/ unlimited User) | ab 1100 Euro/Monat | ab 1000 Euro/Monat | Managed Firewall ab 390 Euro/Monat, Anti-Spam ab 0,80 Euro/ Account | ab 30 Euro/Monat | ab 549 Euro/Monat |
| ISO 17799/BS 7799-2 zertifiziert | ○ | ○ | ● | ○ | ○ | ○ |
| Überwachungszeitraum | 24 x 7 x 365 | 24 x 7 x 365 | 24 x 7 x 365 | 24 x 7 x 365 | bis zu 24 x 7 x 365 | 24 x 7 |
| Unterstützung dynamischer IPs | ● | ● | ○ | ○ | ● | ● |
| Installation zusätzlicher Hardware beim Kunden notwendig | ● im Preis enthalten | ○ | in der Regel nicht, gegebenenfalls im Preis enthalten | kundeneigene Firewall bei Managed Firewall-Service | ● im Preis nicht enthalten | ● Firewall |
| Sichere Verbindung zwischen Kunden- und Control-Center | VPN/SSH für Updates + Log-Transfer, Konfigurations Interface HTTPS | AES-verschlüsselt | ISDN, VPN, SSL-verschlüsselt | immer verschlüsselt | VPN, SSL-verschlüsselt, HTTPS | ISDN, VPN, SSL verschlüsselt |
| **Managed Services** | | | | | | |
| Firewall | ● | ● | ● | ● | ● | ● |
| Intrusion-Detection | ● | nur mittels Firewall-Überwachung | ● | ○ | ● | ○ |
| E-Mail | Antivirus, Spam-Schutz | ○ | Anti-Virus, Spam-Filter | Antivirus, Spam-Schutz | Antivirus, Spam-Schutz, Anti-Porn | Virus-Protection durchFirewall |
| HTTP/S + FTP | Content-Filter, Antivirus, URL-Blocking, Mime-Type-Blocking | ○ | Content-Filter, Antivirus, Application-Data-Scanning | ○ | Content-Filter, Antivirus | Web-Blocker, Content-Filter, Virus-Protection durch Firewall |

ja = ● nein = ○ k. A. = keine Angabe




# Vergleichstest

Die Windows-Bordmittel reichen nicht aus, um LAN-Server und Einzelplatz-PCs sicher gegen Angriffe zu schützen. Hierzu bedarf es Hard- und Software-Lösungen. Die Redaktion der *PC Professionell* hat Virenscanner, Anti-Spyware-Tools, Firewalls und Spam-Filter im Labor getestet und die Schwächen einiger Produkte aufgedeckt.

## INHALT

50 **Client-Virenschutz**
54 **Kammerjäger**
58 **E-Mail-Spam-Filter**
63 **Firewalls mit Löchern**
70 **Spam-Abwehr**

# Client-Virenschutz

**Nach den Angriffen von Blaster, Swen, Sobig & Co ist ein aktiver Virenschutz Pflicht. Doch nicht alle Antivirenprogramme können überzeugen.**

Ralf Nebelo, Britta Widmann

Brandgefährlich sind die Viren der neuen Generation Blaster, Swen und Sobig. Denn diese sind besonders vielseitig und verbreiten sich nicht mehr nur über E-Mails, Internet, Disketten oder USB-Sticks, sondern nutzen neue Infektionskanäle. Den W32.Blaster- alias Lovsan-Virus kann sich jeder schon durch das bloße Herstellen einer Internet-Verbindung einfangen. Ausreichenden Schutz gegen diese Gefahren bieten nicht alle Antivirenprogramme. Die wichtigsten Ergebnisse: Bei den weit verbreiteten Viren (In The Wild, ITW) liegt die Erkennungsleistung auf hohem Niveau. Bei den kaum weniger gefährlichen Trojanern und Archivdateien zeigen einige Programme Schwächen. Die Reparatur infizierter Dateien gelingt häufig nur bei MS-Office-Dokumenten. Andere Dateitypen sind oft nur noch zu löschen.

## Hundert Prozent Treffer

Positiv ist das Ergebnis beim Erkennen der 159 ITW-Viren im Testlabor: Bis auf FP-Win Professional erreicht jedes der elf Programme im Labor der *PC Professionell* eine hundertprozentige Trefferquote. Swen, Sobig und Blaster haben alle Testkandidaten im Griff. Beim Aufspüren von 143 Backdoor-Trojanern sind hingegen größere Unterschiede festzustellen. Die Bestnote erzielt hier Norton Antivirus 2004 mit 97,2 Prozent. Das heißt aber, dass selbst der Marktführer vier gefährliche Malware-Programme übersieht.

Viren verbergen sich häufig in komprimierten Dateien wie ZIP, RAR, CAB und TAR. Aber nur Antiviren Kit 2004 von Gdata und Kaspersky Antivirus Personal Pro entdecken alle 30 Viren, die in sechs Archivdateien unterschiedlichen Formats versteckt wurden. Ähnlich lückenhaft arbeiten die Virenscanner beim Aufspüren von Spyware- und Hacking-Tools. Hier liegt der Bestwert bei geringen acht Treffern, die Norton Antivirus 2004 und F-Secure Internet Security 2004 liefern. Diese schlechten Ergebnisse gehen in erster Linie auf rechtliche Beschränkungen zurück: Ein Virenscanner darf nicht eigenständig jedes Hacking-Utility und jeden Dialer als Malware einstufen. Dies ergibt sich aus den AGBs der Utilitys und Dialer. Anwender, die ihren PC wirksam gegen Malware wie Trojaner, Dialer und Adware schützen wollen, können

## Empfehlungen der Redaktion

**Panda Antivirus Platinum 7**
Der Virenscanner erkennt alle ITW-Viren, ist unschlagbar bei der Vorbeugung und der Wiederherstellung verseuchter Dateien und bietet eine sehr gute Ausstattung.



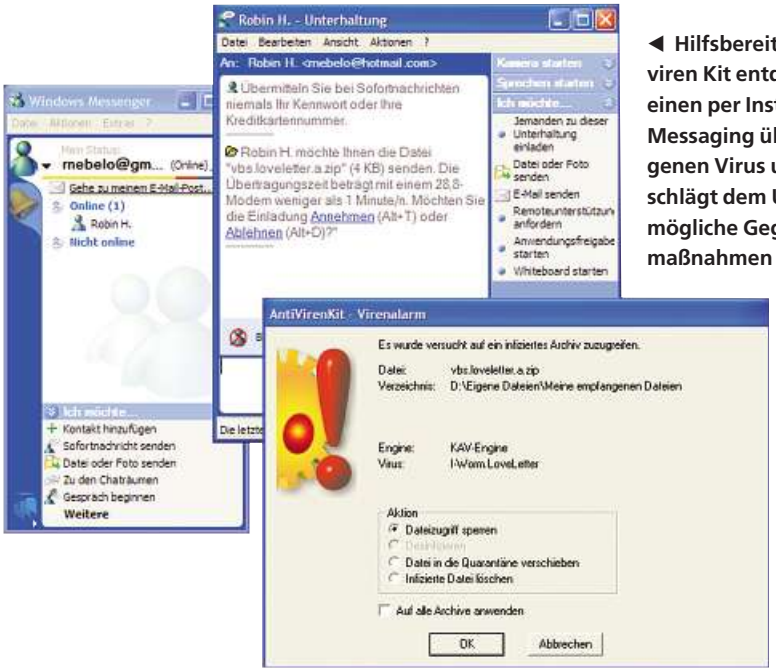

**Norton Antivirus 2004**
Das günstige Symantec-Produkt erzielt die besten Erkennungsraten. In Kombination mit den niedrigsten Update-Kosten ergibt dies das beste Preis-Leistungs-Verhältnis.




| | Produkt Hersteller | (maximal 100 Punkte) |
|---|---|---|
| 1 | **Panda Antivirus Platinum 7** Panda Software | 91,9 |
| 2 | **Norton Antivirus 2004** Symantec | 84,9 |
| 3 | **Antiviren Kit 2004 Professional** Gdata Software | 82,8 |
| 4 | **Antivir Professional 6.21** H+B EDV | 76,2 |
| 5 | **McAfee Virusscan 2004** Network Associates | 69,9 |

das Tool Pestpatrol einsetzen *(www.pestpatrol.com)*. Die Software ist eine gute Ergänzung zum Virenscanner.

Gut funktioniert hingegen die Heuristik der Tools: Bis auf Norman Virus Control, Panda Antivirus Platinum und Antivir Professional erkennen die Scanner auch noch nicht definierte Varianten von bekannten Viren.




**◀ Hilfsbereit: Antiviren Kit entdeckt einen per Instant Messaging übertragenen Virus und schlägt dem User mögliche Gegenmaßnahmen vor.**

## Schlechte Starthilfe im Notfall

Sind wichtige Dateien von einem Virus infiziert, werden professionelle Reparaturen nötig. Die Bereinigung von Office-Dateien beherrscht nahezu jedes Programm im Test – mit Ausnahme von Gdatas Antiviren Kit 2004, das nur drei Excel-Files wiederherstellt. Die restlichen Dateien des Test-Cocktails löschen alle Programme ohne vorherigen Reparaturversuch.

Beim Virenbefall kann es passieren, dass der PC nicht mehr startet. Ein Antiviren-Programm sollte dann über ein startfähiges Notfallmedium verfügen – idealerweise die Programm-CD. Diese ermöglicht die Wiederherstellung von FAT32- und NTFS-5-Partitionen. Aber obwohl alle Programme ausdrücklich als Windows-XP/2000-kompatibel ausgewiesen werden, erlauben nur der Testsieger Panda Antivirus Platinum und Antivir Professional 6.21 die Notfallreparatur einer NTFS-5-Festplatte. Fünf Tools bieten selbst unter Windows-95/98/Me keinerlei Starthilfe für den Pannenfall.

Im Test schaffen Norman Virus Control, Anti-Virus Complete und NOD32 Antivirus System es nicht, eine mit dem Parity-Bootvirus befallene Diskette zu reparieren. Und nur sieben von elf Tools verstehen sich auf den umfassenden Schutz von POP3-Accounts – darunter findet sich Panda Antivirus Platinum. Beim Datei-Download via Internet oder Instant Messaging geben die meisten Wächter nur bei unkomprimierten Viren Alarm. Dafür schlagen einige Programme Alarm, wenn gar kein Virus vorliegt. Die Idealzahl von null Fehlalarmen erreicht im Test nur ein Programm: FP-Win Professional.

## Scanner mit Sandbox

In der Ausstattung geben sich die Tools von Panda, Gdata und H+B EDV keine Blöße. Alle Programme verfügen über einen Echtzeit-Virenwächter sowie automatisierte Scan-Vorgänge. Eine integrierte Firewall, die die Ports des Rechners gegen Wurmattacken à la W32.Blaster schützt, bringen nur Anti-Virus Complete, Antivirus Platinum und F-Secure Internet Security mit, eine Sandbox-Funktion, die Viren in einem geschützten Bereich prüft, sogar nur Norman Virus Control.

Der Einsatz eines leistungsfähigen Antivirenprogramms ist unumgänglich für Anwender, die häufig mailen und im Internet surfen. Lückenlose Sicherheit bietet aber keines der getesteten Programme. User müssen oft mit Firewalls, Malware-Scannern und Anti-Spam-Tools nachrüsten.

## Gratis-Virenschutz

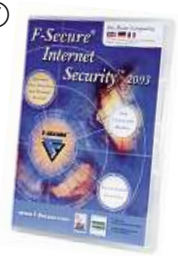
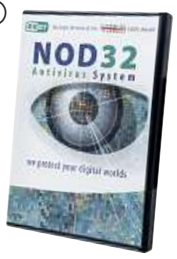
Anwender, die nicht zwischen 35 und 140 Euro für ein Antiviren-Programm ausgeben möchten, finden im Internet eine Reihe kostenloser Alternativen. Dazu gehören Antivir Personal Edition von H+B EDV *(www.free-av.de)* sowie die englischsprachive AVG Anti-Virus 6 Free Edition *(www.grisoft.com/us/us_dwnl_free.php)*. Beide besitzen sowohl einen On-demand-Virenscanner für die gezielte Suche nach Viren auf der Festplatte als auch einen Echtzeit-Virenwächter.

Hinsichtlich der Erkennungs- und Reparaturleistungen brauchen sich die beiden Freeware-Produkte nicht vor kommerziellen Antiviren-Programmen zu verstecken. Es gibt jedoch Einschränkung beim vorbeugenden Schutz etwa von E-Mail-Postfächern, bei Bedienung, Konfigurierbarkeit und beim Support durch den Hersteller. BWI

# Wertung & Ausstattung

| | PLATZ ① | PLATZ ② | PLATZ ③ | PLATZ ④ | PLATZ ⑤ |
|---|---|---|---|---|---|
| |  |  |  |  |  |
| **Hersteller** | Panda Antivirus Platinum 7 | Norton Antivirus 2004 | Antiviren Kit Professional 2004 | Antivir Professional 6.21 | McAfee Virusscan 2004 |
| **Produkt** | Panda Software | Symantec | Gdata Software | H+B EDV | Network Associates |
| **Gesamturteil** [Punkte] | sehr gut 91,9 | gut 84,9 | gut 82,8 | befriedigend 76,2 | befriedigend 69,9 |
| Leistung (50%) [Punkte] | 1. Platz 92,5 | 2. Platz 88,1 | 3. Platz 77,9 | 4. Platz 73,6 | 5. Platz 67,7 |
| Ausstattung (30%) [Punkte] | 1. Platz 93,8 | 2. Platz 72,9 | 2. Platz 84,3 | 2. Platz 84,3 | 10. Platz 59,5 |
| Bedienung/Support (20%) [Punkte] | 4. Platz 87,6 | 1. Platz 94,8 | 2. Platz 92,7 | 8. Platz 70,3 | 3. Platz 91,0 |
| Info | (020 65) 98 76 54 | (021 02) 745 30 | (02 34) 976 20 | (075 42) 50 00 | (089) 370 70 |
| Internet | www.panda-software.de | www.symantec.de | www.gdata.de | www.antivir.de | www.mcafee.de |
| Preis | 70 Euro | 50 Euro | 40 Euro | 140 Euro | 45 Euro |
| Betriebssysteme | Windows 95/98/Me/NT/ 2000/XP | Windows 98/Me/2000/XP | Windows 98/Me/NT/ 2000/XP | Windows 95/98/Me/NT/ 2000/XP | Windows 98/Me/2000/XP |
| **Wiederherstellen** | | | | | |
| Diskette mit Bootsektor-Virus | ● | ● | ● | ● | ● |
| Notfallreparatur FAT32 | ● | ● | ● | ● | ○ |
| Notfallreparatur NTFS 5 | ● | ○ | ○ | ● | ○ |
| **Vorbeugen** | | | | | |
| Prüfung von E-Mail-Anhängen (POP3) | ● | ● | ● | ○ | ● |
| Prüfung von Instant-Messaging-Downloads | ● | ● | ● | ● nur unkomprimiert | ● nur unkomprimiert |
| Prüfung von Internet-Downloads | ● | ● | ● | ● nur unkomprimiert | ● nur unkomprimiert |
| Blockierung von Windows-Skripts | ● | ● | ○ | ○ | ● |
| **Ressourcenverbrauch** | | | | | |
| CPU-Auslastung beim Scannen (Prozent) | 26 | 52 | 67 | 32 | 78 |
| Speicherauslastung beim Scannen (Prozent) | 13 | 13 | 14 | 9 | 11 |
| **Ausstattung** | | | | | |
| Prüft Viren in folgenden getesteten Archivformaten | CAB, EXE, LZH, TAR, ZIP | CAB, EXE, LZH, RAR, TAR, ZIP | CAB, EXE, LZH, RAR, TAR, ZIP | CAB, EXE, LZH, RAR, TAR, ZIP | CAB, EXE, LZH, TAR, ZIP |
| Heuristik | ● | ● | ● | ● | ● |
| Erweiterte Sandbox-Funktionalität | ○ | ○ | ○ | ○ | ○ |
| Echtzeit-Virenwächter | ● | ● | ● | ● | ● |
| Integrierte Firewall | ● | ○ | ○ | ○ | ○ |
| Scheduler | ● | ● | ● | ● | ● |
| Mitgeliefertes Notfall-Bootmedium | ● | ● | ● | ● | ○ |
| Einstellbarer Ressourcenverbrauch | ● | ○ | ● | ● | ○ |
| **Bedienung/Support** | | | | | |
| Integration in Windows-Explorer | ● | ● | ● | ● | ● |
| Online-Update der Virensignaturen | ● | ● | ● | ● | ● |
| Automatisches Update möglich | ● | ● | ● | ● | ● |
| Update-Kosten für 1 Jahr | 50 Euro | 20 Euro | 35 Euro | 115 Euro | 20 Euro |
| Online-Virenübermittlung an Virenlabor über die Programmoberfläche | ● | ● | ● | ● per Diskette | ● |
| (Online-)Virendatenbank | ● | ● | ● | ● | ● |
| Gedrucktes Handbuch | ● | ● | ● | ● | ● |
| Support-Hotline (Telefon) | (020 65) 98 72 50 | (069) 66 41 03 53 | (018 01) 00 11 88[3)] | (075 42) 930 40 | (069) 66 40 43 30 |
| **Fazit** | beste Ausstattung, schützt zuverlässig vor Viren, repariert verseuchte Dateien optimal | beste Erkennungsleistung im Test, niedrigste Update-Kosten | sehr gute Erkennungsleistung, sehr bedienerfreundlich, Schwächen bei der Reparatur | durchschnittliche Erkennungsleistungen, überzeugt bei der Reparatur, Notfallreparatur von NTFS-5-Partitionen möglich | sehr bedienerfreundlich, Scan-Ergebnisse sind unterdurchschnittlich |

● = ja ○ = nein [1)]Auslandstarif [2)]0,12 Euro/Minute [3)]0,05 Euro/Minute [4)]1,86 Euro/Minute

| | PLATZ ⑥ | PLATZ ⑦ | PLATZ ⑧ | PLATZ ⑨ | PLATZ ⑩ | PLATZ ⑪ |
|---|---|---|---|---|---|---|
| |  |  |  |  |  |  |
| | **FP-Win Professional 5.14** | **Internet Security 2003** | **Antivirus Personal Pro 4.5** | **Anti-Virus Complete 7.1** | **Norman Virus Control 5.6** | **NOD 32 Antivirus System** |
| | **Percomp** | **F-Secure** | **Kaspersky** | **Buhl Data** | **Norman Data Defense** | **ESET/Datsec** |
| | **befriedigend 67,7** | **befriedigend 67,5** | **ausreichend 64,6** | **ausreichend 64,3** | **ausreichend 60,9** | **ausreichend 59,4** |
| | 5. Platz 67,7 | 7. Platz 63,5 | 9. Platz 60,3 | 10. Platz 55,4 | 11. Platz 53,1 | 8. Platz 62,0 |
| | 8. Platz 69,1 | 7. Platz 70,9 | 9. Platz 61,4 | 5. Platz 72,9 | 4. Platz 76,6 | 11. Platz 55,7 |
| | 9. Platz 65,4 | 7. Platz 72,4 | 5. Platz 80,2 | 6. Platz 73,5 | 11. Platz 56,7 | 10. Platz 58,6 |
| | (040) 69 62 81 60 | (089) 78 74 67 00 | (+7) 09 57 97 87 00[1] | (018 05) 35 45 51[2] | (02 12) 26 71 80 | (036 41) 637 83 |
| | www.percomp.de | www.f-secure.de | www.kaspersky.com/de | www.buhl.de | www.norman.de | www.nod32.de |
| | 90 Euro | 45 Euro | 100 Euro | 50 Euro | 60 Euro | 40 Euro |
| | Windows 95/98/Me/NT/ 2000/XP | Windows 95/98/Me/NT/ 2000/XP | Windows 95/98/Me/NT/ 2000/XP | Windows 98/Me/NT/ 2000/XP | Windows 95/98/Me/NT/ 2000/XP | Windows 95/98/Me/NT/ 2000/XP |
| | ● | ● | ● | ○ | ○ | ○ |
| | ● | ○ | ○ | ○ | ● | ○ |
| | ○ | ○ | ○ | ○ | ○ | ○ |
| | ○ | ○ | ● nur Outlook | ● | ● | ● |
| | ○ | ● | ○ | ● nur unkomprimiert | ● nur unkomprimiert | ● nur unkomprimiert |
| | ● nur unkomprimiert | ● | ● nur unkomprimiert | ● nur unkomprimiert | ○ | ● nur unkomprimiert |
| | ○ | ○ | ○ | ○ | ○ | ○ |
| | 15 | 49 | 68 | 94 | 49 | 11 |
| | 9 | 11 | 10 | 10 | 12 | 10 |
| | EXE, LZH, TAR, ZIP | CAB, EXE, LZH, RAR, ZIP | CAB, EXE, LZH, RAR, TAR, ZIP | CAB, EXE, LZH, RAR, TAR, ZIP | EXE, ZIP | LZH, RAR, ZIP |
| | ● | ● | ● | ● | ● | ● |
| | ○ | ○ | ○ | ○ | ● | ○ |
| | ● | ● | ● | ● | ● | ● |
| | ○ | ● | ○ | ● | ○ | ○ |
| | ● | ● | ● | ● | ● | ● |
| | ● | ○ | ○ | ○ | ● | ○ |
| | ○ | ○ | ○ | ○ | ○ nur für automatisierte Suchläufe via Scheduler | ○ |
| | ● | ● | ● | ● | ● | ● |
| | ● | ● | ● | ● | ● | ● |
| | ● | ● | ● | ● | ● | ● |
| | 70 Euro | 50 Euro | 80 Euro | 35 Euro | 40 Euro | 27 Euro |
| | ○ | ○ | ● | ● | ○ | ○ |
| | ● | ● | ● | ○ | ● | ● |
| | ● | ● | ● | ● | ○ | ○ |
| | (040) 696 28 16 12 | (089) 787 46 73 00 | (+7) 09 57 97 87 07[1] | (018 05) 35 45 51[2] | (019 08) 722 36[4] | (036 41) 637 83 |
| | kein Konkurrent scannt so schnell; schwacher E-Mail-Schutz, erkennt nicht alle ITW-Viren | gute Erkennungsleistung, Notfalldiskette fehlt, Erstellen einer Notfalldiskette nicht möglich | keine zentrale Einstellmöglichkeit der Scan-Engine, hohe Update-Kosten, hoher Ressourcenverbrauch beim Scannen | große Schwächen bei der Wiederherstellung befallener Dateien, sehr hohe CPU-Auslastung beim Scannen | schlechteste Erkennungsleistungen im Testfeld trotz Sandbox-Funktion | sehr schlechte Wiederherstellungsergebnisse, Ausstattung nicht ausreichend, geringer Ressourcenverbrauch |

# Kammerjäger

**Ad- und Spyware terrorisieren unvorsichtige Internet-Surfer bis zum völligen Stillstand des Rechners. Abhilfe versprechen spezielle Spyware-Scanner.**

Konstantin Breyer

Der Spyware-Terror beginnt gleich nach dem Systemstart. Noch bevor der Desktop zu sehen ist, startet Virtual Bouncer, ein Tool, das als Spyware-Blocker angeboten wird. In Wirklichkeit ist Virtual Bouncer selbst Spyware: Es installiert sich ohne Zustimmung des Users, sendet verschlüsselt User-Daten an seinen Hersteller und lässt sich nur entfernen, wenn der User alle Registry-Einträge und Dateien vollständig manuell entfernt. Spyware ist Software, die im Hintergrund User-Daten an Spammer schickt, Bandbreite stiehlt, um Werbung zu verteilen, und vom Nutzer unbemerkt weitere schädliche Komponenten installiert.

## Sicherheit durch spezielle Tools

Gegen Spyware helfen weder Firewall noch Virenscanner, sondern die Tools im Test: am besten der Testsieger Pestpatrol. Auf dem verseuchten Test-PC, den *PC Professionell* präpariert, sind 634 Schädlinge installiert. Die meisten starten ungefragt beim Windows-Boot-up, so dass der Systemstart wesentlich länger dauert. Versteckte ActiveX-Elemente starten im Hintergrund die Browser-Engine *iexplore.exe* und kommunizieren hierüber mit dem Internet. Frech begründen einige der Werbetreibenden dies so: Die Spyware überträgt Daten an ihren Hersteller, um den User von der Mühe zu entlasten, dies selbst zu tun.

In der Praxis sieht das so aus: Ein Spy-Tool des Typs Browser Helper Object (BHO) hat die Adresseingabe des Internet Explorers so verändert, dass der User den gewünschten URL nun an eine Werbeseite sendet, die den User auf angeblich hierzu passende Informationsseiten führt. Die Suchfunktion ist so verändert, dass alle sonst wählbaren Suchmaschinen wie Google oder Altavista auf eine einzige IP-Adresse umgeleitet werden. Diese zeigt irreführende, meist aus Werbung bestehende Suchergebnisse. Dies nennen Experten Host-Faking. Selbst der Windows-Explorer ist nicht mehr normal nutzbar: Auch hier führt die Eingabeleiste zu Web-Spammern. Aber alle anderen Windows-Funktionen reagieren ebenfalls mit mehr als zehn Sekunden Verzug, denn CPU und RAM sind voll ausgelastet: Im Hintergrund laden nämlich Schädlinge wie das in Kazaa integrierte Tool P2P Networking ständig neue Spionage-Tools aus dem Web herunter. Einige dieser Down-

## Empfehlungen der Redaktion

**Pestpatrol 4.2**
Spyware erkennt und beseitigt Pestpatrol am besten. Pestpatrol liefert zudem sehr gute Sypware-Infos.

PC PROFESSIONELL Empfehlung der Redaktion

PestPatrol

**Spybot Search & Destroy 1.2**
Das kostenlose Spybot erkennt rund 60 Prozent der Spyware-Komponenten und informiert umfangreich über viele Gefahren.

PC PROFESSIONELL Budget Empfehlung

Spybot Search&Destroy

| | Produkt Hersteller | (maximal 100 Punkte) |
|---|---|---|
| 1 | **Pestpatrol 4.2** Pestpatrol | 85,6 |
| 2 | **Ad-Aware Pro 6.1** Lavasoft | 85,6 |
| 3 | **Spysweeper 2.1** Webroot | 81,2 |
| 4 | **Spybot Search & Destroy 1.21** Kolla | 80,2 |
| 5 | **Antispion 4.0** Data Becker | 66,4 |

loads sind als kostenlose PC-Spiele getarnt. Ferner wird Spam über die Leitung des Users an Dritte weitergesendet, die davon ebenso wenig ahnen wie der lokale Benutzer selbst. In entgegengesetzter Richtung übertragen alle Spy-Tools Nutzerdaten: Die harmloseren senden nur die Mail-Adresse des Users oder besuchte Web-Adressen und Formulareingaben, die der Anwender getätigt hat. Andere Tools dagegen senden sehr umfangreiche Ströme, deren Inhalt mit proprietären Verfahren verschlüsselt ist. Was übertragen wird, wissen nur die meist anonymen Programmierer der Tools. Vermutlich handelt es sich um Systemabbilder, die durch Hash-Werte alle installierten Anwendungen sowie Inhalte weiterer Ordner preisgeben. Nur so lässt sich das hohe Transfervolumen logisch erklären. Fazit: Ohne Spyware-Scanner verlieren vor allem User, die sich oft auf Warez- und anderen Untergrundseiten aufhalten, schnell und unbemerkt die Kontrolle über ihren PC und die von ihnen bezahlte Internet-Leitung.

## Sicherheit auf allen Ebenen

Die getesteten Spyware-Scanner untersuchen Arbeitsspeicher, Festplatte und Registry auf Spuren von Spyware. Den größten Erfolg verzeichnet dabei Testsieger Pestpatrol. Das Tool findet und vernichtet fast 80 Prozent der von *PC Professionell* im System versteckten Spione. Auch die Informationen über die gefundene Spyware sind so ausführlich wie bei keinem anderen Scanner. Hier die wichtigsten Tipps für alle, die noch nicht gegen Spyware geschützt sind:

- Zuerst sollten Sie dringend einen Blocker gegen Spyware installieren, bevor zu viele Spione im System lauern. Denn Tools wie Pestpatrol und Spybot Search & Destroy können bereits den Download vieler Schädlinge erkennen und verhindern.
- Zweitens sollte zusätzlich ein Dialer-Blocker mit integrierter Scan- und Entfernungsfunktion eingesetzt werden. Der Dialer-Belastung speziell deutscher Internet-PCs zeigt sich nämlich keiner der getesteten Spyware-Scanner gewachsen. Empfehlenswert sind hierbei beispielsweise YAW 3.5 *(www.yaw.at)* oder 0190/0900-Warner 4.0 *(www.wtrate.de)*.
- Ein wichtiges Mittel zur Vorbeugung ist der Erwerb eines Internet-Werbeblockers. Denn oft wird der getarnte Download von spionierenden ActiveX-Elementen sowie Dialern durch eine Flut von nicht korrekt zu schließenden Werbefenstern eingeleitet oder der User wird gar durch Pop-ups von unbemerkt im Hintergrund installierten Skripts abgelenkt.




**▲ Testsieger: Pestpatrol zeigt dem Anwender ausführliche Informationen zu gefundener Spyware an.**

## Pestpatrol 4.2

Während alle anderen Programme bei gleicher Dateimenge fünf Minuten für ihre Scans brauchen, benötigt der Testsieger dafür stets etwa die doppelte Zeit. Diese sollte der Anwender Pestpatrol aber gönnen. Denn die Ergebnisse können sich sehen lassen. Fast 80 Prozent der Schadanteile im System werden von Pestpatrol erkannt und auf Wunsch beseitigt. Nur bei Web-Dialern zeigt Pestpatrol erhebliche Lücken, wie alle anderen Tools in diesem Test. Unschlagbar ist die ausführliche Dokumentation auf Englisch, aus der selbst Spyware-Experten manches neue Detail erfahren dürften. Dank des integrierten Spyware-Download-Blocker ist auch die Ausstattung weitestgehend vollständig. Die Bedienung ist gut. Eine Online-Aktualisierung hält die integrierte Datenbank mit den Signaturen auf dem neuesten Stand.

## Die häufigsten Datenspione

| Spyware | Weltweite Meldungen (Dezember 2003) |
|---|---|
| 1 GAIN | 221 787 |
| 2 WildTangent | 145 768 |
| 3 KaZaA | 96 742 |
| 4 Ezula | 78 534 |
| 5 Hotbar | 55 963 |
| 6 Cydoor | 25 357 |
| 7 Download Accelerator Plus | 15 586 |
| 8 e-Bates Money Maker | 12 820 |
| 9 LimeWire | 12 766 |
| 10 Golden Palace Casino | 11 076 |

Quelle: Pestscan *(www.pestpatrol.com)*

### Ad-Aware 6.1 Pro

Fast 13 000 Erkennungsmuster hält das seit Jahren kontinuierlich verbesserte Ad-Aware bereit. Doch zumindest im realistisch aufgebauten Test-Mix von *PC Professionell* erkennt Ad-Aware gut fünf Prozent weniger gefährliche Komponenten im Testsystem als Pestpatrol, das mit weniger Suchmustern auskommt. Dafür bietet Ad-Aware eine bessere Bedienung gegenüber Pestpatrol. Bis auf den fehlenden Download-Blocker gegen Spyware ist auch die Ausstattung weitgehend vollständig.

### Spysweeper 2.1

Einen ebenfalls hohen Anteil der im Testsystem versteckten Spyware, nämlich fast 71 Prozent, erkennt das nur wenigen Kennern vertraute Tool Spysweeper. Mit Platz drei knapp hinter den bekannten Tools von Pestpatrol und Lavasoft und noch vor Spybot ist das Programm ein Neuzugang im internationalen Spitzenfeld. Neben der Leistung überzeugt auch die durchweg übersichtliche Bedienung. Lediglich die Ausstattung ließe sich an einigen Punkten optimieren. So fehlt etwa ein Blocker gegen Spyware-Downloads.

### Spybot Search & Destroy 1.2

Durch seine mit gut 60 Prozent ordentliche Spyware-Vernichtungsrate überzeugt das kostenlose Spybot. Die zum Teil außerordentlich gelungene Dokumentation zeigt allerdings zu manchen gefundenen Tools noch nicht gefüllte Info-Kästchen an. Sinnvoll ist hingegen der Hinweis im Programm, dass zahlreiche Programme ohne ihre Spyware-Komponenten nicht mehr genutzt werden dürfen. Zu der durchweg überzeugenden Ausstattung zählt außerdem ein Blocker gegen Spyware-Downloads.

### Antispion 4.0

Das gut bedienbare Tool findet im Test rund ein Drittel der vorhandenen Spyware. Trotz aktueller Updates werden viele Spione und deren Komponenten nicht erkannt. Von 2000 Spy-Dateien bleiben über 1400 im System zurück, darunter viele, die unbemerkt neue Spyware aus dem Netz laden. Am Funktionsumfang des Tools lässt sich lediglich aussetzen, dass nicht bereits Spyware-Downloads erkannt und gestoppt werden. Data Becker sollte die Menge der beim Scan erfassten Spyware erhöhen. Dann kann Antispion zur Spitzengruppe der Programme im Test aufschließen. KBR

## Wertung & Ausstattung

PLATZ ① PestPatrol — PC Professionell Empfehlung der Redaktion — PLATZ ② LAVASOFT

| Produkt | | Pestpatrol 4.2 | Ad-Aware Pro |
|---|---|---|---|
| **Hersteller** | | **Pestpatrol** | **Lavasoft** |
| **Gesamturteil** | [Punkte] | **gut 85,6** | **gut 85,5** |
| Leistung (60 %) | [Punkte] | 1. Platz 90,9 | 2. Platz 86,7 |
| Bedienung (20 %) | [Punkte] | 5. Platz 70,0 | 1. Platz 90,0 |
| Ausstattung (20 %) | [Punkte] | 1. Platz 85,0 | 4. Platz 77,5 |
| Info | | (07 81) 929 32 22 | (02 21) 31 08 80 |
| Internet | | www.pestpatrol.com | www.lavasoft.de |
| Preis | | 37 Euro | 40 Euro, mit Registry-Editor 60 Euro |
| **Ausstattung** | | | |
| Unterstützte Betriebssysteme | | Windows 95/98/Me/NT 4/ 2000/XP | Windows 98/Me/NT 4/2000/XP |
| Voraussetzungen CPU, RAM | | Pentium/133, 32 MByte RAM | Pentium/100, 64 MByte RAM |
| Log-Funktion | | ● | ● |
| Statistik unerwünschter Aktivitäten | | ● | ● |
| Blockieren unerwünschter Verbindungen | | ● unerwünschte Downloads | ○ |
| Löschen unerwünschter Dateien | | ● | ● |
| Ausnahmen konfigurierbar | | ● | ● |
| Wiederherstellungsfunktion | | ● | ● |
| Registry-Editor | | ● | ● |
| Zusatzfunktionen | | bekämpft Keylogger und 48 andere Schädlingsarten | bekämpft Browser Helper Objects (Hijacker) und ActiveX-Malware |
| **Wirkungsbereiche** | | | |
| Adware | | ● | ● |
| Pop-ups | | ○ | ○ |
| Unsichtbare Webgrafiken | | ○ | ○ |
| Dialer | | ● ausgewählte | ● ausgewählte |
| Trojaner | | ● | ● ausgewählte |
| Würmer | | ● | ● ausgewählte |
| Cookies mit Tracking | | ● | ● |
| **Service** | | | |
| Handbuch | | ● HTML | ● HTML |
| Live-Update | | ● | ● |
| Wizard | | ● | ● |
| Support via Web | | ● FAQ, Helpdesk | ● FAQ |
| Support per Telefon | | ○ | ○ |
| Support per Mail | | helpdesk.pestpatrol.com | pro@lavasoft.de |
| Weitere Versionen | | Small Business (ab 23 Euro), Corporate (ab 23 Euro) | Standard (kostenlos), Plus (27 Euro) |
| Gleiches Produkt verfügbar unter folgenden Namen | | BHV Spionage-Abwehr (40 Euro) | ○ |
| **Fazit** | | entfernt viele Spyware-Komponenten, liefert viele Infos | am besten bedienbar im Test, entfernt die zweithöchste Zahl von Spionen |

● = ja ○ = nein [1)]Auslandstarif

| | PLATZ ③ | PLATZ ④ | PLATZ ⑤ | PLATZ ⑥ | PLATZ ⑦ | PLATZ ⑧ |
|---|---|---|---|---|---|---|
| | Spysweeper 2.1 | Spybot Search & Destroy 1.2 | Antispion 4.0 | Spyremover 1.30d | Spy-Killer 2.1 | Adware Agent 3.1b |
| | Webroot | Kolla | Data Becker | Infoworks | Maxion | Killer |
| | gut 81,2 | gut 80,2 | befriedigend 66,4 | ausreichend 62,0 | ausreichend 59,0 | mangelhaft 43,2 |
| | 3. Platz 84,6 | 4. Platz 76,6 | 6. Platz 54,5 | 5. Platz 55,7 | 7. Platz 54,0 | 8. Platz 37,1 |
| | 2. Platz 87,0 | 3. Platz 86,0 | 3. Platz 86,0 | 5. Platz 73,0 | 7. Platz 68,0 | 8. Platz 52,0 |
| | 6. Platz 65,0 | 1. Platz 85,0 | 3. Platz 82,5 | 5. Platz 70,0 | 6. Platz 65,0 | 8. Platz 52,5 |
| | (001) 30 34 42 38 13[1)] | (02 34) 68 72 68 79 | (02 11) 933 18 00 | (001) 41 26 35 92 24[1)] | webmaster@maxion software.com | support@killersoftware.com |
| | www.webroot.com | security.kolla.de | www.databecker.de | www.itcompany.com | www.maxionsoftware.com | www.killersoftware.com |
| | 28 Euro pro Jahr | kostenlos | 20 Euro | 23 Euro | 46 Euro | 15 Euro |
| | Windows 98/Me/NT 4/ 2000/XP | Windows 95/98/Me/NT 4/ 2000/XP | Windows 98/Me/2000/XP | Windows 95/98/Me/NT 4/ 2000/XP | Windows 95/98/Me/NT 4/ 2000/XP | Windows 98/Me/2000/XP |
| | Pentium/150, 32 MByte RAM | Pentium/100, 64 MByte RAM | Pentium II/300, 128 MByte RAM | Pentium/75, 32 MByte RAM | Pentium/100, 64 MByte RAM | Pentium/100, 64 MByte RAM |
| | ● | ● | ● | ● | ● | ○ |
| | ○ | ● | ● | ● | ● | ○ |
| | ○ | ● unerwünschte Downloads | ○ | ○ Zusatztool Spystopper (23 Euro) | ● unerwünschte Downloads | ○ |
| | ● | ● | ● | ● | ● | ● |
| | ● | ● | ● | ● | ● | ● |
| | ● | ● | ● | ● | ● | ○ |
| | ○ | ○ | ○ | ○ | ○ | ○ |
| | bekämpft Keylogger, entfernt Nutzerspuren | bekämpft Dialer, Browser Helper Objects (Hijacker), Keylogger, ActiveX- und andere Malware, entfernt Nutzerspuren, Direktzugriff auf Windows Registry-Editor | bekämpft Browser Helper Objects (Hijacker), Keylogger, ActiveX- und andere Malware, entfernt Nutzerspuren | Direktzugriff auf Windows Registry-Editor | arbeitet auch im Stealth-Mode (versteckt), bekämpft Keylogger, blockt Installation von rund 230 verschiedenen Schädlingen | bekämpft Browser Helper Objects (Hijacker) und ActiveX-Malware |
| | ● | ● | ● | ● | ● | ● |
| | ○ | ○ | ● | ○ | ○ | ○ |
| | ○ | ○ | ○ | ○ | ○ | ○ |
| | ○ | ● | ● ausgewählte | ● ausgewählte | ● ausgewählte | ● ausgewählte |
| | ● | ● ausgewählte | ● ausgewählte | ● ausgewählte | ○ | ● ausgewählte |
| | ○ | ● ausgewählte | ○ | ○ | ○ | ● ausgewählte |
| | ● | ● | ● | ● | ○ | ○ |
| | ● HTML | ● HTML | ● gedruckt | ● HTML | ● HTML | ○ |
| | ● | ● | ● | ● | ● | ● |
| | ● | ● | ● | ● | ● | ● |
| | ● FAQ | ● FAQ | ● Security-Check | ● FAQ | ○ | ○ |
| | ○ nur für US-Kunden | ○ | (02 11) 933 16 66 | ○ | ○ | ○ |
| | support@webroot.com | www.safer-networking.org/index.php?lang=en&page=contact-new | ○ | support@itcompany.com | webmaster@maxion software.com | support@killersoftware.com |
| | ○ | ○ | ○ | ○ | ○ | ○ |
| | ○ | ○ | abgeleitet von Bulletproof Spyware Adware Remover | abgeleitet von Spybot Search & Destroy | ○ | ○ |
| | intuitiv bedienbar, entfernt viel Spyware, spartanische Ausstattung | gut ausgestattete Freeware mit zufrieden stellendem Scanner und reichhaltigen Informationen | durchweg gut bedienbar und gut ausgestattet, erkennt aber zu wenig aktuelle Spione | erkennt rund ein Drittel der aktuellen Spione, Bedienung ist mittelmäßig | rundum schwache Einzelleistungen, die Bedienerführung ist noch akzeptabel | inakzeptable Leistungen, nur sieben von 100 Spyware-Komponenten werden gefunden |

# E-Mail-Spam-Filter

**Bis zu 50 Prozent aller Mails sind Spam: Nur mit der passenden Software können Anwender mit hohem Mail-Aufkommen die Werbeflut eindämmen.**

Daniel Dubsky

Die Flut von Spam-Mails nimmt bedrohliche Ausmaße an: Seit Juli 2003 wird täglich schon genau so viel Spam versandt wie reguläre Mails, schätzen Forscher von Messagelabs *(www.messagelabs.com)*. Immerhin 500 Millionen deutschsprachiger Junkmails werden pro Woche verschickt, so das Institut Marketagent *(www.marketagent.com)*. Diese unverlangten Werbemails kosten den Anwender Zeit, Bandbreite und damit Geld. Zudem sind Junk-Mails ein Sicherheitsrisiko. Nicht selten enthalten sie Viren oder Spyware oder fordern den Empfänger gar auf, sensible Informationen wie etwa Kreditkartennummern und Log-in-Daten herauszugeben.

Ratschläge, die Mail-Adresse geheim zu halten oder regelmäßig zu wechseln, sind nicht praxisnah. Spam lässt sich dadurch zwar reduzieren, aber nicht ganz ausschließen. Hierzu bedarf es spezieller Filterprogramme. Neben den in Mail-Clients integrierten Filtern gibt es eine Reihe von Antispam-Tools. 9 solcher Tools unter 20 Euro testet *PC Professionell:* Testsieger ist das kostenlose Spam Pal 1.53, das mithilfe aktueller Plug-ins eine gute Spam-Erkennung erreicht.

## Individuell filtern

Das Hauptproblem von Spam-Blockern ist die Unterscheidung, welche Mail Spam ist und welche nicht: Eine technische Definition von Spam existiert nicht. Da jeder Nutzer andere Interessen hat, können Mails, die einige Anwender informativ finden, von vielen anderen als Spam klassifiziert werden. Daher muss auch ein guter Spamfilter vom User angepasst werden. In den Default-Einstellungen mithilfe der mitgelieferten Filter-Regeln und Blacklists erreichen alle Spam-Blocker im Test nur unzureichende Ergebnisse: Der Großteil der unverlangten Mail gelangt weiterhin in die Inbox, oder es werden neben Spam auch viele erwünschte Mails gelöscht. Mit unterschiedlich hohem Aufwand können die meisten Tools im Test Spam komplett blocken. Doch es sollten keine wichtigen Mails im Spamfilter hängen bleibt.

## Anwender müssen nachbessern

Bei guten Tools bekommt der Benutzer fertige Filter-Listen zum Programm oder auf Nachfrage vom Autor zugesandt. Der Benutzer

## Empfehlung der Redaktion

**Farmer Spam Pal 1.53**

In der Standardinstallation fragt das kostenlose Spam Pal Online-Listen von Spam-Sendern ab, so genannte DNSBL-Listen. Durch kostenlose Plug-ins wird es um lernfähige Bayesische Filter, URL-Checker und einen HTML-Modifier, der Web-Bugs unschädlich macht, ergänzt und ist so für Spammer kaum überwindbar. Ist Spam Pal richtig konfiguriert, arbeitet es mit minimaler Pflege im Hintergrund.

PC PROFESSIONELL Empfehlung der Redaktion

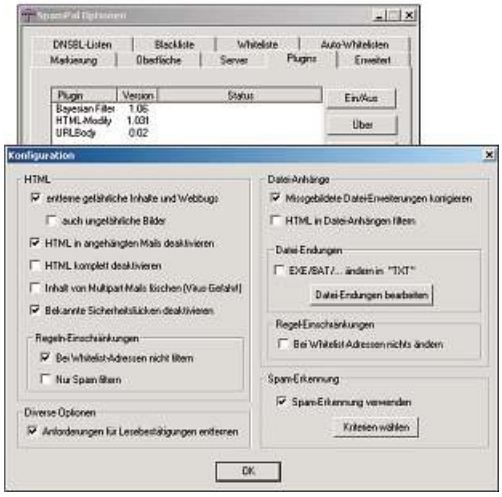
SpamPal FOR WINDOWS

| | Produkt Hersteller | (maximal 100 Punkte) |
|---|---|---|
| 1 | **Spam Pal 1.53** Farmer | 84,9 |
| 2 | **Pac Spam Pro 6.41** Heitho | 84,4 |
| 3 | **Spamihilator 0.9** Krämer | 82,3 |
| 4 | **Super Spam Killer Pro 3.15** Boer | 78,5 |
| 5 | **Anti Spam 1.0** SAD | 69,8 |

muss seine Regeln, Blacklists und Whitelists aber zunächst pflegen, bevor er gute Ergebnisse erreicht und den Filter nicht mehr nach fehlgefilterten Mails (so genannten False Positives) durchsuchen muss. Dieser Aufwand ist vor allem für User mit hohem Mail-Aufkommen sinnvoll. Wer nur wenig Mails bekommt, ist meist schneller, wenn er unerwünschte Post manuell löscht.

Die meisten Tools im Test laden lediglich die Header der Mail herunter und analysieren die Mail danach auf Spam-Verdacht. Hat der Benutzer den Entscheidungen des Programms zugestimmt oder diese korrigiert, können die Mails bereits auf dem Server gelöscht werden, auch bei POP3-Accounts. So können User, deren Online-Zugang nach Zeit und Transfervolumen abgerechnet wird, Übermittlungskosten sparen. Erst wenn dies erledigt ist, lädt der Client die verbliebenen Mails herunter.

Spam Pal und andere Tools hingegen markieren Mails als Spam, nachdem sie zwischen Mail-Client und POP3-Server Inhalte und Adressen geprüft haben. Der Benutzer sieht also alle Mails, die er bekommen hat, und muss nicht befürchten, dass versehentlich etwas gelöscht wird. Die weitere automatisierte Behandlung der markierten Mails kann etwa Outlook übernehmen und Spam-verdächtige Mails im Ordner *Gelöschte Objekte* ablegen. Allerdings gelingt es im Test keinem Filter, Spam und Mail absolut genau zu unterscheiden. Dafür nutzen Spam-Versender zu oft neue Tricks und Mail-Adressen. Doch wer einen Spam-Blocker mit gut konfigurierbaren Filtern nutzt, kann schnell reagieren und Regeln erstellen, um nicht erkannte Absender und Betreffzeilen auszusondern.




**▲ Testsieger Spam Pal bekämpft Junkmail mit DNSBL-Listen, lernfähigen Filtern und URL-Checker. Ein HTML-Modifier schützt vor Web-Bugs.**

Fort und Zeitersparnis steht die zweite Gruppe: Die leistungsstarken Tools Spam Pal und Spamihilator sowie das deutlich weniger wirksame Tool De Spam Tunnel. Jede Anfrage des Mail-Clients wird an den Filter weitergeleitet, der Mails abruft und prüft. Mails werden bei Spam-Verdacht lediglich markiert und in die Mail-Client-Inbox gestellt. Testsieger Spam Pal sollte nach der Installation durch kostenlose Plug-ins, um Filter und Regeln erweitert werden. Spam Pal fragt in der Grundeinstellung nur DNSBL-Listen über Spam-Versender ab, was allein mäßig wirksam ist. Das Tool bringt aber zusätzlich die besten Werkzeuge für eine genaue Konfiguration durch User mit und erzielt nach dieser die beste Blockwirkung im Test.

In den Grundeinstellungen sind alle Tools wenig wirksam, neun Tools halten dann auch manche erwünschte Mail für Spam. Wichtig ist daher eine Positivliste (Whitelist).

Auch das Gegenstück zur Whitelist, die Blacklist, hat Nachteile. Enthaltene Spammer ändern oft ihre Adressen. Um gleich ganze Domains zu sperren, muss der User sicher sein, von dort keine persönlichen Mails zu erwarten. Doch zur Abwehr von Spam-Newslettern ist eine Blacklist gut geeignet. Bei De Spam Tunnel fehlt diese. Zudem kann der User bei fünf Tools die Blacklist nur über Regeln für einzelne zu sperrende Absender anlegen. Das ist nicht nutzerfreundlich und in der Praxis zu umständlich gelöst. KBR

## Kaum Schutz ohne Blocker

In den meisten E-Mail-Clients sind nur sehr einfache Spamfilter integriert oder sie fehlen gänzlich. Brauchbar sind der Spamschutz von Mozilla Thunderbird *(thunder bird.die-pause.de)* und Outlook ab Version 2003.

Die Spam-Tools im Test lassen sich in zwei Gruppen einteilen. Zur ersten gehören als wirksamste Tools Pac Spam Pro und Super Spam Killer Pro. Ferner gehören Anti Spam, Mail Cleanup, Spam Flush dazu. Solche Tools verwalten die Einstellungen für Mailserver und rufen die Mails nach Anweisung des Nutzers oder automatisiert ab. Dies eignet sich für User, die Bandbreite sparen wollen. Mailheader werden heruntergeladen und analysiert. Der User muss meist das Interface des Spam-Blockers nutzen, um Entscheidungen des Filters zu prüfen. Für mehr Komfort und Zeitersparnis steht die zweite Gruppe: Die leistungsstarken Tools Spam Pal und Spamihilator sowie das deutlich weniger wirksame Tool De Spam Tunnel. Jede Anfrage des Mail-Clients wird an den Filter weitergeleitet, der Mails abruft und prüft. Mails werden bei Spam-Verdacht lediglich markiert und in die Mail-Client-Inbox gestellt. Testsieger Spam Pal sollte nach der Installation durch kostenlose Plug-ins, um Filter und Regeln erweitert werden. Spam Pal fragt in der Grundeinstellung nur DNSBL-Listen über Spam-Versender ab, was allein mäßig wirksam ist. Das Tool bringt aber zusätzlich die besten Werkzeuge für eine genaue Konfiguration durch User mit und erzielt nach dieser die beste Blockwirkung im Test.

In den Grundeinstellungen sind alle Tools wenig wirksam, neun Tools halten dann auch manche erwünschte Mail für Spam. Wichtig ist daher eine Positivliste (Whitelist).

Auch das Gegenstück zur Whitelist, die Blacklist, hat Nachteile. Enthaltene Spammer ändern oft ihre Adressen. Um gleich ganze Domains zu sperren, muss der User sicher sein, von dort keine persönlichen Mails zu erwarten. Doch zur Abwehr von Spam-Newslettern ist eine Blacklist gut geeignet. Bei De Spam Tunnel fehlt diese. Zudem kann der User bei fünf Tools die Blacklist nur über Regeln für einzelne zu sperrende Absender anlegen. Das ist nicht nutzerfreundlich und in der Praxis zu umständlich gelöst. KBR

## Empfehlenswert: Spam Bully 2 für Outlook

Vollständig in Outlook ab Version 2000 integriert, prüft dieser Spamfilter von Axaware *(www.spambully.com)* alle eingerichteten POP3-, IMAP- und sogar Hotmail-Konten auf unerwünschte Nachrichten. Nach der Installation werden alle in Outlook vorhandenen Outlook-Kontakte und Mail-Empfänger automatisch als vertrauenswürdig eingestuft. Neue Mails werden auf Grundlage eines Bayesian-Filters analysiert. Außerdem ist es möglich, Absender aus bestimmten Ländern und Mails in fremden Sprachen generell als Spam zu klassifizieren. Spam Bully kann auch Informationen aus Realtime-Blackhole-Listen (RBL) beziehen. Sie können zudem eigene Filter definieren und einen Trainingsmodus starten. Enthalten sind Statistiken und eine Funktion zum Aktivieren von geblockten Dateianlagen. Das Zusammenspiel der Spam-Abwehrtechniken führt bei rund 7000 Test-Nachrichten zu einer Erkennungsquote von über 99 Prozent von richtigen Unterscheidungen zwischen Spam und erwünschten Mails.Die 25 Euro teure Software verdient sich in den Kriterien Leistung, Ausstattung und Bedienung durchweg sehr gute Noten.

# Wertung & Ausstattung

| | | PLATZ ① | | PLATZ ② | | PLATZ ③ | | PLATZ ④ | |
|---|---|---|---|---|---|---|---|---|---|
| **Produkt** | | **Spam Pal 1.53** | | **Pac Spam Pro 6.41** | | **Spamihilator 0.9.6** | | **Super Spam Killer Pro 3.15** | |
| **Hersteller** | | **Farmer** | | **Heitho** | | **Krämer** | | **Böer** | |
| **Gesamturteil** | [Punkte] | **gut** | **84,9** | **gut** | **84,4** | **gut** | **82,3** | **befriedigend** | **78,5** |
| Wirksamkeit (60 %) | [Punkte] | 2. Platz | 88,0 | 1. Platz | 88,4 | 2. Platz | 88,0 | 5. Platz | 78,3 |
| Bedienung (30 %) | [Punkte] | 1. Platz | 85,9 | 6. Platz | 74,0 | 5. Platz | 75,1 | 3. Platz | 80,0 |
| Kompatibilität (10 %) | [Punkte] | 10. Platz | 63,3 | 1. Platz | 91,7 | 5. Platz | 70,0 | 4. Platz | 75,0 |
| Info | | jjf@spampal.twinlobber.org.uk | | (053 51) 42 41 07 | | michel@undercouch.de | | info@wt-rate.com | |
| Internet | | www.spampal.de | | www.heitho.de | | www.spamihilator.com | | www.superspamkiller.de | |
| Preis | | kostenlos | | 15 Euro | | kostenlos | | 15 Euro | |
| **Filter** | | | | | | | | | |
| Schlüsselwörter/Regeln/beides im- und exportierbar | | ○/○/○ | | ●/●/● | | ●/○/○ | | ●/●/● | |
| Blacklist/Whitelist/DNSBL-Listen | | ●/●/● | | ○ nur Einzelregeln/●/○ | | ●/●/○ | | ○ nur Einzelregeln/●/● | |
| Vordefinierte Filter/Filter-Update per Web/eigene Filter definierbar | | entfällt, da Abfrage von | | ●/○/● | | ●/○/● | | ●/○/● DNSBL-Listen im Web | |
| Filterstärke variierbar | | ○ | | ○ | | ● | | ○ | |
| **Programm** | | | | | | | | | |
| Kann Mail auf Server löschen/nur markieren/herunterladen und löschen | | ○/●/○ | | ●/○/○ | | ○/○/● | | ●/○/○ | |
| Bounce/Abuse/Whois | | ○/○/○ | | ●/●/● | | ○/○/○ | | ●/○/○ | |
| Postfach-Import/vordefinierte Mail-Anbieter/mehrere Konten zu verwalten | | ○/○/● | | ○/●/● | | ●/○/● | | ●/○/● | |
| Unabhängig vom Mail-Client/unterstützt Hotmail/AOL | | ●/○/○ | | ●/○/○ | | ●/○/○ | | ●/●/● | |
| Fragt POP3-Server ab/leitet Outlook-Anfragen an POP3-Server weite | | ○/● | | ●/○ | | ○/● | | ●/○ | |

| | | PLATZ ⑤ | | PLATZ ⑥ | | PLATZ ⑦ | |
|---|---|---|---|---|---|---|---|
| **Produkt** | | **Anti Spam 1.0** | | **Mail Cleanup 5 2.3.0 SR 1** | | **De Spam Tunnel** | |
| **Hersteller** | | **SAD** | | **Steganos** | | **De-Nu** | |
| **Gesamturteil** | [Punkte] | **befriedigend** | **69,8** | **ausreichend** | **60,9** | **ausreichend** | **62,5** |
| Wirksamkeit (60 %) | [Punkte] | 8. Platz | 60,4 | 7. Platz | 61,5 | 6. Platz | 68,5 |
| Bedienung (30 %) | [Punkte] | 2. Platz | 82,5 | 8. Platz | 62,5 | 12. Platz | 44,9 |
| Kompatibilität (10 %) | [Punkte] | 2. Platz | 88,3 | 7. Platz | 68,3 | 10. Platz | 63,3 |
| Info | | (073 05) 962 90 | | (08 00) 78 34 26 67[1)] | | du-ne@web.de | |
| Internet | | www.s-a-d.de | | www.steganos.com | | www.gcf.de/du-ne/despam | |
| Preis | | 15 Euro | | 16 Euro | | kostenlos | |
| **Filter** | | | | | | | |
| Schlüsselwörter/Regeln/beides im- und exportierbar | | ●/●/● | | ●/●/○ | | ●/○/○ | |
| Blacklist/Whitelist/DNSBL-Listen | | ●/●/○ | | ○ nur Einzelregeln/○/○ | | ○/●/○ | |
| Vordefinierte Filter/Filter-Update per Web/eigene Filter definierbar | | ●/○/● | | ●/○/● | | ●/○/● | |
| Filterstärke variierbar | | ○ | | ○ | | ● | |
| **Programm** | | | | | | | |
| Kann Mail auf Server löschen/nur markieren/herunterladen und löschen | | ●/○/○ | | ●/○/○ | | ○/●/○ | |
| Bounce/Abuse/Whois | | ●/○/○ | | ●/●/○ | | ○/○/○ | |
| Postfach-Import/vordefinierte Mail-Anbieter/mehrere Konten zu verwalten | | ●/●/● | | | | ●/○/● | |
| Unabhängig vom Mail-Client/unterstützt Hotmail/AOL | | ●/○/○ | | ●/○/○ | | ●/○/○ | |
| Fragt POP3-Server ab/leitet Outlook-Anfragen an POP3-Server weiter | | ●/○ | | ●/○ | | ○/● | |

● = ja ○ = nein [1)]gebührenfrei

## Nicht im Test

Angesichts der gut funktionierenden und zugleich kostenlosen Spam-Filterprogramme sind die kommerziellen Lösungen Symantec Antispam 2004 *(www.symantec.de)* und McAfee Spamkiller 5.0 *(www.mcafee.com)* mit Preisen von jeweils 40 Euro zu teuer – zumal das Abonnement der entsprechenden Anti-Spam-Signaturen auf ein Jahr begrenzt ist. Anti-Spamware von IOK *(www.antispam-ware.de)* bietet zum Preis von 30 Euro zwar eine sehr gute Ausstattung mit AOL- und Hotmail-Unterstützung, fällt aber ebenfalls durch das Preisraster, das die Redaktion mit 20 Euro festlegt. Daher werden die genannten Programme von der Redaktion nicht im Test berücksichtigt.

# Neue Antispam-Technologien

**Selbstständig lernende Filter, nur einmal gültige E-Mail-Adressen und Spam-Blocker nach dem Peer-to-Peer-Prinzip sollen das Spam-Problem zukünftig lösen und die Postfächer der Empfänger bereinigen.**

Daniel Dubsky

Spam ist für die jeweiligen Absender eine preiswerte Werbemethode: Fast unbegrenzt viele Adressen können zu geringen Kosten bedient werden. Diese trägt der Empfänger in Form von Zeitaufwand und Entgelt für zusätzliche Bandbreite. Auch korrekte Mail-Adressen, wie sie etwa Quadress *(www.quadress.de)* ab 10 Cent pro Empfänger anbietet, brauchen Spammer nicht unbedingt. Viele Adressen werden per Software mit Wortlisten (etwa unter *packetderm.cotse.com/wordlists)* künstlich generiert und ausprobiert.

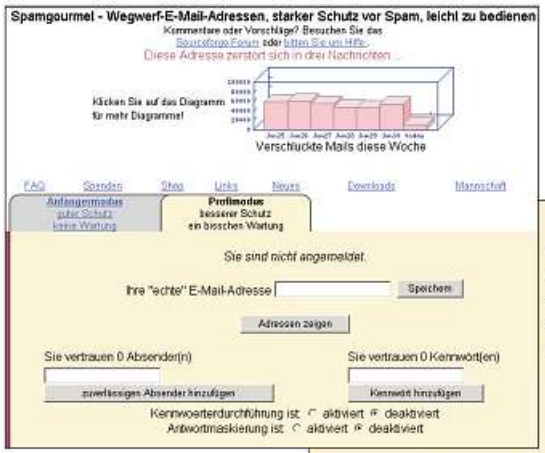
## Höhere Hürden gegen Spam

Mail-Provider integrieren ständig zusätzliche und bessere Anti-Spam-Filter – die Belastung für User bleibt dennoch hoch, wie das folgende Beispiel zeigt. Seit Ende 2002 setzt etwa MSN Hotmail auf eine Technik, die es Spammern erschwert, automatisiert neue Accounts anzulegen. Ferner gilt eine Grenze von 100 verschickbaren Mails pro Tag und User. Seit Herbst 2002 kooperiert Microsoft zudem mit Brightmail, einem Anbieter von Antispam-Technologie. Die verwendeten Filter entfernen Spam am SMTP-Server, bevor dieser die Mails weiterleitet. Die Filter basieren auf Tests mit 200 Millionen Mail-Adressen.

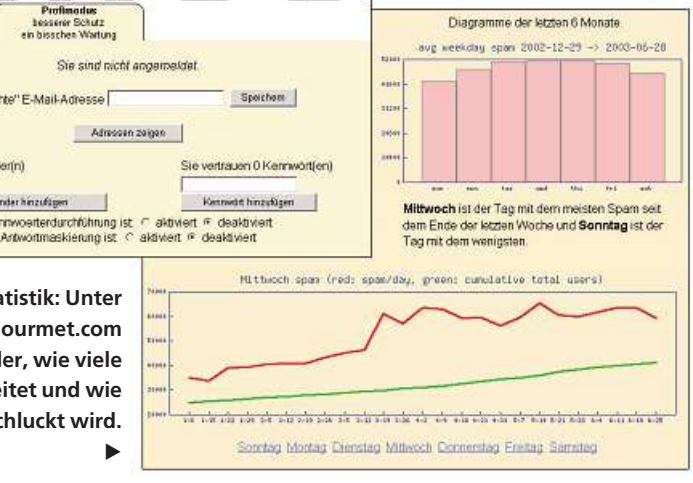
Hotmail erkennt nach eigenen Angaben täglich 2,4 Milliarden Spam-Mails, das wären 80 Prozent des gesamten Mail-Aufkommens bei MSN. Das ist kaum nachprüfbar, weil der User den Anteil des Spam, der den Mailserver gar nicht erst erreicht, nicht messen kann. MSN unterbindet die automatische Bildansicht in Mails. Das verhindert, dass unsichtbare 1-Pixel-Bilder (Web Bug oder Web Beacons genannt) dem Spam-Versender das Lesen der Mail bestätigen. Die Grafik wird hierbei nicht per HTTP eingebunden, zum Beispiel mit *<img src="http://web-adresse.tld/bild.gif">*, sondern via FTP nachgeladen. Als Log-in wird die Mail-Adresse übermittelt *<img src="ftp://anonymous:mail-adresse@ftp. server name.tld/bild.gif">*. Ist die Mail-Adresse als aktiv bestätigt, wird sie wertvoller und möglicherweise weiterverkauft. Um diese Spionage auszuschließen, sollten Sie im Mail-Client die HTML-Ansicht deaktivieren. Vor allem sollten nie Links in Spam-Mails angeklickt werden, da diese häufig mit Zahlenkombinationen gekoppelt sind und ebenfalls dem Verifizieren von Mail-Adressen dienen.

## Listen schwarzer Schafe

Spammer setzen Mails meist über öffentlich zugängliche SMTP-Server ab (Open Relays) oder verwenden Spezial-Software, um dies von dynamischen IPs aus zu tun. Da ein weltweites Schließen offener Server und die Kontrolle von Einwahl-IPs unrealistisch sind, erstellen Organisationen Listen solcher Server und IPs. Diese heißen DNSBL (Domain Name Service Blackhole List). Mails, die von eingetragenen IPs kommen, werden als Spam erkannt. Ist ein Mailserver an DNSBL angeschlossen, weist er die Mail zurück. Das spart dem User Ressourcen. Doch auch wichtige Mails, die von einer solchen IP kommen, werden blockiert. Ein Beispiel: Die dynamische Q-DSL-IP 212.202.193.191 ist in den meisten DNSBL-Listen als Spam-Sender erfasst. Doch jeder Q-DSL-User mit dynamischer IP kann diese IP jederzeit zugewiesen bekommen und




◀ **Werden in Web-Formularen Mail-Adressen verlangt, sind Wegwerf-Adressen die Lösung – wie hier bei Spamgourmet.**




**Spam-Statistik: Unter www.spamgourmet.com sehen Anwender, wie viele Mails weitergeleitet und wie viel Spam geschluckt wird.** ▶

wird dann als Spammer zurückgewiesen. DNSBL-Listen finden sich unter anderem auf *spamcop.net* und *relays.osirusoft.com*. Wer wissen will, ob seine IP-Adresse in den Listen steht, erfährt das unter *openrbl.org*. Wie schwer es ist, sich aus einer DNSBL-Liste auszutragen, erfuhr GMX Ende Mai, als die Open-Relay-Database *(ordb.org)* die GMX-Server testete: Dabei gelang es, von einigen GMX-Adressen Mails auch ohne eine Authentifizierung abzusetzen. Viele Server wiesen daraufhin via GMX versandte Mails automatisch ab.

Spamfilter analysieren dagegen den Inhalt der Mail. Vor allem der Header wird hier geprüft. Bestimmte Zeichenketten im Betreff, etwa Leerzeichen, Großbuchstaben und sinnlose Zeichenketten gelten als Hinweis auf Spam. Weitere sind fehlerhafte und erdachte Absender-Domains sowie ein leeres Adressfeld. Letzteres kann aber auch aufgrund von Blindkopie-Versand leer sein. Deshalb werden Filter um Black- und Whitelists ergänzt, die Ausnahmen definieren.

Eine neue Art der Spam-Erkennung leisten Bayes-Filter. Diese analysieren Wörter in Mails und die Wahrscheinlichkeit, dass die Mail Spam ist. Das erfordert einen langen Lernprozess, in dem viele Mails durchlaufen. Ist der Filter eingespielt, sind die Erkennungsraten hoch. Manche Programme, etwa die Open-Source-Software Spam Assassin *(www.spamassassin.org)* kombinieren verschiedene Techniken.

## Spam per P2P bekämpfen

Das Peer-to-Peer-Prinzip (P2P) nutzt Cloudmark *(www.cloudmark.com)* im Filter Spamnet. Die Nutzung kostet 4 Euro im Monat, die Betaversion ist allerdings kostenlos. Spamnet integriert sich als Menüleiste in Outlook. Wer Junkmails erhält, kann den Button *Block* wählen, woraufhin Spamnet eine Prüfsumme der Mail errechnet und diese online weitergibt. Jede Mail hat eine andere Prüfsumme. Bei allen Spamnet-Nutzern landet diese Mail nun im Spam-Ordner. Ein leistungsfähiger Filter entsteht, wenn viele User Spam so filtern. Private Mails bleiben fast nie im Filter hängen. Da diese in der Regel nur an einen Nutzer gehen, kann kein anderer die Prüfsumme dieser Mail im Netz verteilen.

Mailinglisten sind dann relativ sicher, wenn sie ausschließlich an User versenden, die sich eingetragen haben. Um Sabotage zu verhindern, nutzt Spamnet ein Rating: Wer oft Nicht-Spam als Spam meldet, wird vom System nach einer Weile ignoriert.




**▲ Spamnet erkennt dank P2P-Austausch über 91,3 Prozent des Spam im Test – ohne dass der Anwender hierfür komplizierte Regeln erstellen muss.**

## Wegwerf-Adressen

Damit Spammer nicht an echte Adressen gelangen, gibt es Wegwerf-Adressen. Auf Websites lassen sich Adressangaben zwar durch Formulare umgehen. Da aber im Impressum eine Mail-Adresse stehen muss, werden Adresssammler dort fündig. Auch eine ASCII-Codierung der Mail-Adresse bietet nur wenig Schutz, da Such-Tools (Spam-Bots) diese mittlerweile erkennen. Hier wie bei allen Diensten, die eine gültige Mail-Adresse erfordern, beispielsweise um ein Passwort zuzusenden, helfen Einwegadressen: Ein kostenloser Anbieter ist Spamgourmet *(www.spamgourmet.com)*, es gibt jedoch weitere wie etwa das *PC-Professionell*-Utility Centermail *(www.lab1.de)*. Der Benutzer registriert sich mit einer Mail-Adresse, an die der Dienst dann die erhaltenen Mails weiterleitet. In der Basisvariante von Spamgourmet kann der Anwender festlegen, wie viele Mails an eine Adresse geschrieben werden können. Die Adresse hat die Form *variabler_teil.zahl.benutzername@spamgourmet.com*. Der erste Teil ist frei wählbar und dient der Unterscheidung der Adressen, *zahl* gibt an, wie viele eintreffende Mails (maximal 20) diese Adresse akzeptiert. Der Clou: Adressen müssen nicht angelegt werden. Das tut Spamgourmet automatisch, sobald eine Mail an die Adresse eintrifft.

Mit Source-Authentication arbeitet Blockallspam (*www.blockallspam.com*, 10 Euro). Der Mail-Sender erhält von Blockallspam eine Antwort, die er bestätigen muss. Nur dann wird seine Nachricht zugestellt. KBR

# Firewalls mit Löchern

**Viele Hersteller wiegen User in trügerischer Sicherheit: Harte Angriffe aus dem Internet und Tricks von Trojanern hebeln die meisten Software-Firewalls aus.**

Konstantin Breyer

Die meisten Hersteller preisen ihre Firewalls vollmundig an. Marktführer Symantec etwa verspricht auf der gelben Packung seiner Norton Personal Firewall 2004: Das Programm »hält Hacker fern und persönliche Daten unter Verschluss« und auf der Rückseite wird erklärt, dass »Spyware-Programme und Trojanische Pferde nicht unbemerkt Daten an das Internet senden« können. Symantec, aber auch fast alle anderen Firewalls werden solchen Versprechen im Test nicht gerecht. Einzig der englischsprachige Testsieger Sygate Personal Firewall 5.5 Pro, jetzt als deutsche Sprachversion bei BHV *(www.bhv.de)* erschienen, blockt im Test alle gefährlichen Angriffe ab.

## Alternative: Hardware-Firewalls

Daneben parieren acht getestete Hardware-Firewalls unter 350 Euro im Test alle Hacker-Attacken mit hohem Gefahrenpotenzial. Unter diesen Geräten ist Zyxel Zywall 2 Testsieger. Hardware-Firewalls sind zwar für User, die täglich über eine Stunde online sind, ein unverzichtbarer Schutz gegen Hacker. Doch sie helfen nicht gegen Trojaner, die vom PC aus persönliche Daten an Spione im Internet versenden. Damit diese geblockt werden, sollten User auf jeden Fall eine Desktop-Firewall einsetzen, egal wie lange sie online sind.

## Trojaner senden unerkannt

Um zu testen, ob die Software wirklich Trojaner am Senden hindert, setzt *PC Professionell* drei gängige Simulationen ein, die jede Desktop-Firewall durchschauen sollte: Dabei versuchen Programme, vom User-PC aus unter falschen Namen Daten ins Internet zu senden. Zum Beispiel tarnt sich die Simulation Firehole als Internet Explorer. Obwohl die meisten Firewalls versprechen, dass dank ihrer Hilfe Trojaner nicht nach Hause telefonieren können, enttarnen nur die Firewalls Sygate, Kerio und Tiny diese drei Testangriffe. Norman, Internet Security Alliance und Agnitum/Buhl Fire Alarm fallen zumindest jeweils nur auf einen der Angriffe Firehole, Leaktest und Tooleaky herein. Alle anderen Firewalls, darunter bekannte Programme wie beispielsweise Mc Afee, Symantec und Zone Alarm, lassen mindestens zwei dieser drei Angriffe unerkannt passieren.

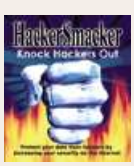
## Empfehlungen der Redaktion: Software-Firewall-Lösungen

**Sygate Personal Firewall 5.5 Pro**
Die Software-Firewall lässt keinem der über 1800 getesteten Hacker-Angriffe und keinem geprüften Trojaner-Angriff eine Chance.



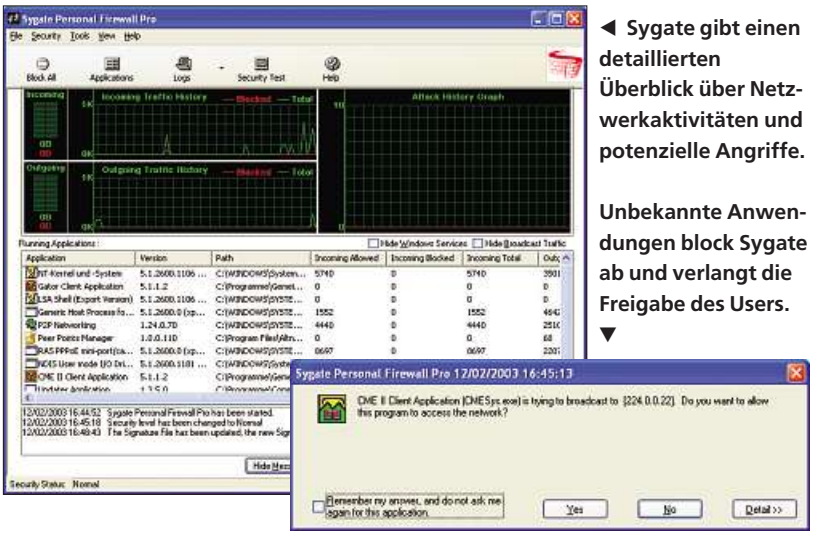

PC PROFESSIONELL Empfehlung der Redaktion

**Farstone Hackersmacker 1.14**
Gegen Hack-Angriffe von außen schützt die mit 19 Euro besonders günstige Firewall tadellos, hier ist das Tool Spitze.




PC PROFESSIONELL Budget Empfehlung

| | Produkt Hersteller | (maximal 100 Punkte) |
|---|---|---|
| 1 | **Sygate** Personal Firewall 5.5 Pro | 84,5 |
| 2 | **Norman** Personal Firewall | 79,5 |
| 3 | **Farstone** Hackersmacker 1.1 | 73,4 |
| 4 | **NAI** Mc Afee Personal Firewall Plus | 67,8 |
| 5 | **Terminet** NT Kernel Personal Firewall | 66,1 |




**◀ Sygate gibt einen detaillierten Überblick über Netzwerkaktivitäten und potenzielle Angriffe.**

**Unbekannte Anwendungen block Sygate ab und verlangt die Freigabe des Users. ▼**

## Test mit 1800 Hacker-Angriffen

Während auf den PC geschleuste Trojaner von innen angreifen, um persönliche Daten des Users nach draußen an ihren Nutznießer zu senden, dringen klassische Hacker-Angriffe von außen über das Internet ein. Über 1800 verschiedene Attacken mit verschiedenen Gefährlichkeitsgraden legen im *PC-Professionell*-Test offen, wie gut die Firewalls Hackern standhalten. Bei den Hardware-Firewalls zeigen hier nur vier von zwölf Geräten Probleme: Draytek lässt einen gefährlichen Angriff durch, Linksys und SMC je zwei, Longshine hingegen fünf.

Neben acht Geräten bestehen auch 11 von 24 Software-Firewalls alle Test-Hacks in der höchsten Gefahrenklasse ohne Fehler. Dies sind neben Sygate: Hackersmacker und Freedom Firewall, aber auch Terminet, Kaspersky, Internet Security Alliance, Sphinx, Omniquad, ISS Black Ice, Cyber Firewall 2003 von Pearl sowie die Deerfield-Firewall. Mit nur einem Fehler bei den gefährlichsten Angriffen liefern Norman, Mc Afee und Symantec immerhin weitgehenden Schutz gegen Hack-Attacken. Alle anderen Testkandidaten lassen fünf oder mehr gefährliche Angriffe durch und sind daher nicht zu empfehlen.

Neben den genannten Tests führt *PC Professionell* unter anderem Prüfungen mit Spyware durch und testet, ob die Firewalls das Surfen beeinträchtigen.

## Produke im Detail

Nicht nur Hacker-Angriffe und Trojaner machen vielen Firewalls im Test erheblich zu schaffen. Auch Spyware stellt ein ungelöstes Problem für die meisten Firewalls am Markt dar. Denn Malware wie Gator beschädigt nicht nur das Windows-System nachhaltig, sondern dient dazu, persönliche Daten auszuspionieren und via Web zu verschicken.

Zwar bieten Spezialtools wie Pestpatrol *(www.blitzbox.de)* Schutz . Doch obwohl es sogar gute Freeware wie Ad-aware *(www.lavasoftusa.com)* und Spybot Search & Destroy *(www.safer-networking.org)* gibt, setzen noch viel zu wenige User diese Spyblocker ein. Um so wichtiger ist es, dass Firewalls Gator, Cydoor, Gain und ähnliche Spione wenigstens daran hindern, die ausspionierten Daten an ihre Hintermänner im Internet zu schicken. Nur die ansonsten wenig überzeugende Firewall Armor 2 Net integriert einen Spyblocker und entfernt alle vier im Test geprüften Spione vom PC. Sieben weitere Firewallprogramme erkennen zumindest die zwei verbreiteten Spione Gator und Gain. Dies sind neben Testsieger Sygate 5.5 Pro: Norman, Freedom Firewall, Kaspersky, Internet Security Alliance, Sphinx und Surfsecret. Das Besorgnis erregende ist aber: Keine Firewall außer Armor 2

## Empfehlungen der Redaktion: Hardware-Firewall-Lösungen

**Zyxel Zywall 2**
Alle gefährlichen Hackerangriffe via Internet fehlerlos zu blocken, ist für eine gute Hardware-Firewall wie Zywall 2 selbstverständlich. Zudem ist die Einrichtung einfach.

**3Com Cable/ DSL Secure Gateway 4**
Mit 135 Euro Preisempfehlung ist die Firewall extrem günstig. Zudem sind via Web-Interface wertvolle Profi-Features erreichbar.

PC PROFESSIONELL Empfehlung der Redaktion

PC PROFESSIONELL Budget Empfehlung

| | Produkt | Hersteller | (maximal 100 Punkte) |
|---|---|---|---|
| 1 | **Zyxel** | Zywall 2 | 89,9 |
| 2 | **Netgear** | FR 328 S | 88,3 |
| 3 | **3Com** | Cable/DSL Secure Gateway | 87,4 |
| 4 | **Checkpoint** | Safe@Office 105 | 86,3 |
| 5 | **D-Link 4** | DI-804 HV | 86,2 |

Net weist den User darauf hin, dass dies schädliche Spyware ist. Vielmehr fragen die Firewalls ganz neutral an, ob der User einer Anwendung namens Gator Zugang zum Internet gewähren möchte oder nicht. Trotz der Hemmnisse des Wettbewerbsrechts sollten die Hersteller Wege finden, den User hier deutlicher zu warnen.

## Wichtig: Firewall richtig bedienen

Wer sich als Anfänger mit dem Testsieger Sygate anfreunden will, findet in dem Buch »Persönliche Firewalls« eine Einstiegshilfe (Mick Tobor, Markt & Technik, *www.mut.de*, ISBN 38272266569, 20 Euro). Neben Sygate und anderen Firewalls wird auch NAIs Mc Afee Firewall (Platz 4 im Test) besprochen. Diese ist übrigens im Test neben Kerio und Symantec am verständlichsten zu bedienen.

Bei der Auswertung des Netzwerk-Traffics können übrigens alle Hersteller von der in diesem Punkt nahezu optimalen deutschen Agnitum-Version Buhl Fire Alarm lernen.

Eine Sonderrolle hat Terminet NT Kernel Firewall. Diese läuft in der Microsoft Management Console und blockt Hacker-Angriffe nahezu perfekt. Gegen Trojaner und Spyware hilft Terminet nicht, da ein Application Filter fehlt. Viele Windows-User dürften sich wünschen, dass Microsoft dieses Tool statt der vergleichbaren Windows XP Firewall mitliefert, da letztere sechs hochgefährliche und 11 sonstige Hack-Attacken im Test einlässt.

## Surfen ohne Einschränkung

Häufig ärgern sich User, weil ihre Desktop-Firewalls das Surfen im Web beeinträchtigen. Unter anderem ist von älteren Sygate-, Symantec- und Zone-Alarm-Versionen bekannt, dass etwa beim Online-Banking, bei Ebay-Auktionen und während Flash-Animationen mit Cookies Web-Dokumente nicht oder nur fehlerhaft erscheinen. Für betroffene User könnte sich der Neukauf einer Firewall lohnen, denn hier zeigen die meisten Programme Verbesserungen. Lediglich bei Tiny 5.0 lassen sich nennenswerte Probleme auf Flash-Sites mit Cookies feststellen. Ob die eigene Homebanking-Site oder eine andere wichtige URL durch eine Firewall gut erreichbar ist, kann jeder User selbst mit einer Trial-Version der Firewall testen.

Keinen Grund zur Klage bieten auch die Geschwindigkeitsmessungen, die *PC Professionell* bei allen Firewalls vornimmt. Gegenüber einem ungeschützten System verlangsamen die aktuellen Programme die im Test genutzte




**◀ Während Norman die Trojan-Simulation Tooleaky kar blockiert, weist Mc Afee Gator nicht als Spyware aus. ▼**

1&1-DSL-Verbindung durchschnittlich nur um 0,6 bis 2 KByte/s. Da das System ohne Firewall 92,25 KByte/s erreicht, gehen selbst im schlimmsten Fall nur gut zwei Prozent Bandbreite verloren. Die getesteten Hardware-Firewalls kosten den Anwender noch weniger Bandbreite als die Software-Pendants, nämlich nur 0,45 bis 0,7 KByte/s.

Einige der getesteten Firewalls, darunter Testsieger Sygate und Zone Alarm, gibt es in kostenlosen Versionen. Im Test sind aber immer die Bezahlversionen. Denn die Freeware-Versionen verzichten auf wichtige Features, und der User kann kaum verlangen, dass eine kostenlose Firewall vom Hersteller ständig aktuell gehalten wird.

## Sichere Hardware

Da das sehr empfehlenswerte Gerät Trend Micro Gatelock X200 nicht mehr im Vertrieb ist, existiert keine preisgünstige Hardware-Firewall mit integriertem Virenschutz im Testfeld. Gegen Online-Hacker-Angriffe schützen sieben Geräte nahezu perfekt. Bei diesen ist lediglich die meist harmlose Trace-route-Verfolgung bis zum Gerät möglich, alle anderen rund 1800 Angriffe werden souverän geblockt. Diese Geräte kommen von 3Com, Allnet, Billion, Checkpoint, D-Link, Netgear und Test-

## Diese Firewalls sind nicht im Test

Ausgeschlossen sind Programme, die nicht unter Windows XP laufen: beispielsweise Bitguard, Look N Stop, Preventon, Privatefirewall 3.0 und Sillico Seringa. Die Firewall von Webroot ist identisch mit Sygate, Computer Associates EZ Firewall mit Zone Alarm. Ferner werden Suiten inklusive Virenscanner, wie Aladdin Esafe, F-Secure Internet Security 2004 und Trend Micro PC-Cillin 11 nicht aufgenommen.

Ausgeschlossen ist ferner Hardware mit WLAN-Anschluss sowie solche, die nicht PPPoE sowie die Filterung per Stateful Inspection beziehungsweise Stateful Packet Inspection unterstützt. Ansonsten sind im Test alle 24 Standalone-Firewalls für Windows XP, wenn möglich in deutscher Version, sowie 12 Hardware-Firewalls bis 350 Euro, die sich per Browser-Interface ohne Zusatzprogramme einrichten lassen.

sieger Zyxel. Auch die Firewall Bingo DSL von Bintec besteht den Test mit nur zwei harmlosen Fehlern. Das mit 350 Euro teuerste Gerät im Test ist allerdings schlecht bedienbar.

## Nicht alltagstauglich

Auch die Firewalls von Draytek, Linksys, Longshine und SMC lassen sich mit entsprechendem Aufwand sicher konfigurieren. Doch hier beschränkt dies den User beim Nutzen von LAN und Internet, und das zum Teil erheblich. Diese Firewalls sind daher für den Alltag nicht zufrieden stellend gerüstet. Das erstklassig ausgestattete Draytek 2600 X hat wie Zywall 2 und Billion ein DSL-Modem eingebaut und schützt auch ISDN-Verbindungen. Doch Draytek blockt bei normaler Konfiguration weder einen Angriff auf Port 135, mit dem ein Hacker bestimmte ungepatchte Windows-Systeme übernehmen kann, noch den UPNP-Scan auf Port 1900 (Securityspace SS 10829 und 11835, *www.securityspace.com*). Zudem gelangen diverse weniger gefährliche Angriffe zum Erfolg. Auch Linksys und SMC lassen je zwei Angriffe durch bei gängiger Konfiguration für ein kleines LAN. Bei Linksys sind die Denial-of-Service-Attacke Winsyslog und Jolt 2 (SS 11884 und 11902) erfolgreich, bei SMC lassen sich ein Bind-9-Overflow (SS 11318) sowie eine SNMP-Lücke (SS 10264) trotz Firewall ausnutzen. Bei Longshine lassen sich sogar fünf schwere Angriffe durchführen, das ist indiskutabel. Bei Linksys und SMC findet der User, will er alle Angriffe blocken, wegen der ungenügenden Einstellmöglichkeiten nur Funktionen, die auch seine eigene LAN-Nutzung behindern. Ein Fehler von SMC ist ferner, dass der Hersteller Usern empfiehlt, die Standard-Einstellungen nicht zu ändern: Mit diesen bleibt die Firewall deaktiviert, im Test ist die Hacker-Simulation mit mindestens acht Angriffen erfolgreich.

## Tipps für Profis

Wer die 100 bis 350 Euro für eines der Geräte im Test sparen will und einen nicht mehr benötigten PC zur Verfügung hat, kann auch seine eigene Linux-Hardware-Firewall aufsetzen. Mit der kostenlosen Software Smoothwall ist dies schon auf einem 486er-SX-PC mit 32 MByte RAM und 415 MByte Festplattenspeicher möglich *(www.smoothwall.org)*. Spezielle Linux-Kenntnisse sind nicht erforderlich, doch der Anwender sollte sich ausgesprochen gut bei Firewall- und LAN-Themen auskennen. KBR

# Wertung & Ausstattung – Software-Firewalls

| | | PLATZ ① | PLATZ ② | PLATZ ③ |
|---|---|---|---|---|
| **Produkt** | | **Personal Firewall 5.5 Pro** | **Personal Firewall** | **Hackersmacker 1.1** |
| **Hersteller/Vertrieb** | | **Sygate (Vertrieb: BHV)** | **Norman** | **Farstone** |
| **Gesamturteil** | [Punkte] | **gut 84,5** | **befriedigend 79,5** | **befriedigend 73,4** |
| Leistung (75 %) | [Punkte] | 1. Platz 90,0 | 2. Platz 80,4 | 3. Platz 74,0 |
| Ausstattung (15 %) | [Punkte] | 10. Platz 68,7 | 4. Platz 83,3 | 12. Platz 66,0 |
| Bedienung (10 %) | [Punkte] | 8. Platz 67,2 | 8. Platz 67,2 | 4. Platz 79,5 |
| Info | | (021 31) 765 01 | (02 12) 26 71 80 | (+33) 01 43 63 16 75[1] |
| Internet | | www.bhv.de | www.norman.de | www.farstone.com |
| Preis | | 34 Euro | 36 Euro | 19 Euro |
| kostenlose Version verfügbar | | ● | ○ | ○ |
| Einschränkungen kostenlose Version | | ohne IDS, Spoofingschutz, Support | ○ | ○ |
| **Ausstattung** | | | | |
| Application Level Filter/ Packet Level Filter/Stateful Inspection | | ●/●/● | ●/●/○ | ●/●/○ |
| Intrusion Detection (IDS)/ Stealth-Mode für Ports | | ●/● | ●/● | ●/● |
| Blockt Banner/Pop-ups/Flash-Ads | | ○/○/○ | ●/●/○ | ○/○/○ |
| Blockt Skripte/ActiveX/Cookies | | ○/○/○ | ●/●/● | ○/○/○ |
| Autodetect Programme durch Hash-Wert/Autodetect Netzwerk | | ○/● | ●/● | ●/● |
| Log nach Verbindung/Port/Programm/ filterbar/speicherbar | | ●/●/●/●/● | ●/●/●/●/● | ●/●/○/○/● |
| Passwort-geschützt/Live-Update | | ●/○/● | ●/● | ●/○ |
| Hotline | | (021 31) 765 01 | (019 08) 722 36[2] | ○ |
| Sonstige Ausstattung | | ○ | ○ | ○ |
| Fazit | | schützt gegen alle Hacker- und Trojan- sowie wichtige Spyware-Attacken | schützt gegen die meisten Hacker-, Cracker- und Spyware-Angriffe | schützt gut gegen Hacker sowie einige Trojans und Spyware |

| | | PLATZ ⑩ | PLATZ ⑪ | PLATZ ⑫ |
|---|---|---|---|---|
| **Produkt** | | **Norton Personal Firewall 2004** | **The Green Bow Firewall** | **PC Internet Patrol 2.2** |
| **Hersteller/Vertrieb** | | **Symantec** | **Sistech** | **Internet Security Alliance** |
| **Gesamturteil** | [Punkte] | **ausreichend 61,2** | **ausreichend 59,6** | **ausreichend 57,8** |
| Leistung (75 %) | [Punkte] | 14. Platz 53,2 | 8. Platz 61,2 | 10. Platz 58,0 |
| Ausstattung (15 %) | [Punkte] | 3. Platz 87,3 | 19. Platz 56,0 | 17. Platz 57,3 |
| Bedienung (10 %) | [Punkte] | 1. Platz 82,0 | 19. Platz 53,1 | 16. Platz 56,8 |
| Info | | (021 02) 745 30 | (+33) 143 12 39 30[1] | (+1) 24 87 23 50 56[1] |
| Internet | | www.symantec.de | www.thegreenbow.com | www.pcinternetpatrol.com |
| Preis | | 50 Euro | 29 Euro | 84 Euro |
| kostenlose Version verfügbar | | ○ | ○ | ○ |
| Einschränkungen kostenlose Version | | ○ | ○ | ○ |
| **Ausstattung** | | | | |
| Application Level Filter/ Packet Level Filter/Stateful Inspection | | ●/●/● | ●/○/○ | ●/●/○ |
| Intrusion Detection (IDS)/ Stealth-Mode für Ports | | ●/● | ●/● | ●/● |
| Blockt Banner/Pop-ups/Flash-Ads | | ○/●/● | ○/○/○ | ○/○/○ |
| Blockt Skripte/ActiveX/Cookies | | ●/●/● | ○/○/○ | ○/○/○ |
| Autodetect Programme durch Hash-Wert/Autodetect Netzwerk | | ●/● | ○/○ | ●/● |
| Log nach Verbindung/Port/Programm/ filterbar/speicherbar | | ●/●/●/●/● | ●/●/○/○/○ | ○/○/○/○/○ |
| Passwort-geschützt/Live-Update | | ○/● | ●/● | ○/○ |
| Hotline | | (021 02) 745 30 | ○ | ○ |
| Sonstige Ausstattung | | ○ | ○ | ○ |
| Fazit | | zeigt für Trojaner Lücken, blockt die meisten Hacker- und Spyware-Attacken | mittlerer Schutz, schlecht bedienbar, ein Absturz | hält diverse wichtige Angriffe ab, versagt aber gegen Spyware |

● = ja ○ = nein [1]Auslandstarif [2]1,86 Euro pro Minute [3]gebührenfrei [4]0,12 Euro pro Minute

| PLATZ 4 | PLATZ 5 | PLATZ 6 | PLATZ 7 | PLATZ 8 | PLATZ 9 |
|---|---|---|---|---|---|
| **Mc Afee Personal Firewall Plus** | **NT Kernel Personal Firewall** | **Freedom Firewall** | **Personal Firewall 5.0** | **Anti-Hacker 1.5** | **Personal Firewall 4.0** |
| **Network Associates** | **Terminet** | **Zero Knowledge** | **Tiny** | **Kaspersky (Vertrieb: Koch Media)** | **Kerio** |
| befriedigend 67,8 | befriedigend 66,1 | befriedigend 65,2 | ausreichend 64,3 | ausreichend 64,0 | ausreichend 62,6 |
| 5. Platz 62,8 | 4. Platz 67,6 | 5. Platz 62,8 | 5. Platz 62,8 | 8. Platz 61,2 | 13. Platz 54,8 |
| 4. Platz 83,3 | 14. Platz 64,7 | 8. Platz 73,3 | 11. Platz 68,0 | 6. Platz 76,0 | 1. Platz 89,3 |
| 1. Platz 82,0 | 15. Platz 57,4 | 6. Platz 70,9 | 7. Platz 70,3 | 8. Platz 67,2 | 3. Platz 81,4 |
| (089) 370 70 | vadim@ntkernel.com | (+1) 51 43 50 75 53[1] | (+1) 40 89 19 73 60[1] | (08 41) 88 19 71 70 | (+42) 03 77 33 89 01[1] |
| de.mcafee.com | www.terminet.co.za | www.freedom.net | www.tinysoftware.com | www.kaspersky.com/de | www.kerio.com |
| 39 Euro | 42 Euro | 34 Euro | 33 Euro | 50 Euro | 38 Euro |
| ○ | ○ | ○ | ○ | ○ | ○ |
| ○ | ○ | ○ | ○ | ○ | ○ |
| ●/●/● | ○/●/● | ●/●/○ | ●/●/● | ●/●/○ | ●/●/● |
| ●/● | ●/● | ●/● | ●/● | ●/● | ●/● |
| ○/○/○ | ○/○/○ | ○/●/● | ○/○/○ | ○/○/○ | ●/●/● |
| ○/○/○ | ○/○/○ | ●/●/● | ○/○/○ | ○/○/○ | ●/●/● |
| ●/● | ○/○ | ●/○ | ●/○ | ●/● | ●/● |
| ●/●/●/●/● | ●/●/○/○/○ | ●/●/●/○/● | ●/●/●/●/● | ●/●/●/●/● | ●/○/○/●/○ |
| ○/● | ○/○ | ○/● | ●/○ | ○/● | ●/○ |
| (08 00) 100 52 62 2) | ○ | ○ | ○ | (018 05) 65 60 08 3) | (+44) 87 07 44 22 05 |
| ○ | ○ | ○ | Remote-Verwaltung möglich | ○ | ○ |
| blockt fast alle Hacker-Angriffe, kaum Schutz gegen Trojans und Spyware | schützt gut vor Hackern, aber nicht vor Trojans und Spyware | gut gegen alle wichtigen Hacks, viele Spytools und einige Trojaner | gut gegen Trojaner und manche Spyware, viele Lücken gegen Hacker | schützt gegen die meisten Hacker-Angriffe und Spyware, aber nicht gegen Trojaner | schützt gegen Trojaner, Lücken gegen Hacker, aber gut einzurichten |

| PLATZ 13 | PLATZ 14 | PLATZ 15 | PLATZ 16 | PLATZ 17 | PLATZ 18 |
|---|---|---|---|---|---|
| **Sphinxwall 2.0.011** | **Personal Firewall Professional** | **Black ICE PC Protection 3.6** | **Fire Alarm** | **Cyber Firewall 2003** | **Visnetic Firewall 2.1.2** |
| **Sphinx** | **Omniquad** | **ISS (Vertrieb: BVRP)** | **Buhl Data** | **Cybersec (Vertrieb: Pearl)** | **Deerfield** |
| ausreichend 56,5 | ausreichend 55,3 | ausreichend 51,6 | mangelhaft 46,4 | mangelhaft 45,7 | mangelhaft 43,1 |
| 10. Platz 58,0 | 12. Platz 56,4 | 15. Platz 50,0 | 18. Platz 34,0 | 16. Platz 43,6 | 17. Platz 38,8 |
| 21. Platz 49,3 | 23. Platz 52,7 | 13. Platz 65,3 | 2. Platz 88,0 | 22. Platz 50,7 | 20. Platz 54,7 |
| 20. Platz 56,2 | 17. Platz 51,2 | 24. Platz 43,2 | 5. Platz 76,5 | 18. Platz 54,3 | 13. Platz 58,0 |
| sphinxwall@sphinx-soft.com | (+44) 20 87 43 80 93[1] | (089) 790 97 90 | (018 05) 35 45 51[4] | (018 05) 55 82[4] | (+1) 98 97 32 88 56[1] |
| www.sphinx-soft.com | www.omniquad.com | www.bvrp.com | www.buhl.de | www.pearl.de | www.deerfield.com |
| 21 Euro | 33 Euro | 34 Euro | 50 Euro | 30 Euro | 13 Euro |
| ○ | ● | ○ | ● (www.agnitum.com) | ○ | ○ |
| ○ | ohne IP-Tracking, IP-Blocking, Einzelport-Regeln | ○ | ohne Stateful Inspection, Auto-Detect, Flash-Ad-Blocker, Passwortschutz | ○ | ○ |
| ●/○/○ | ●/●/○ | ●/●/● | ●/●/○ | ●/○/○ | ○/●/● |
| ●/● | ●/● | ○/● | ●/● | ●/● | ●/● |
| ○/○/○ | ○/○/○ | ○/○/○ | ●/●/● | ○/○/○ | ○/○/○ |
| ○/○/○ | ○/○/○ | ○/○/○ | ●/●/● | ○/○/○ | ○/○/○ |
| ●/○ | ○/○ | ●/● | ●/● | ●/○ | ○/○ |
| ○/○/○/○/○ | ●/○/●/○/○ | ○/○/○/○/○ | ●/●/●/●/● | ●/●/●/○/● | ○/○/○/○/● |
| ○/○ | ○/○ | ○/○ | ●/● | ○/○ | ●/○ |
| ○ | (+44) 20 87 43 80 93[1] | (+33) 141 83 44 66[1] | ○ | (018 05) 55 82[4] | 150 Euro Aufpreis |
| ○ | ○ | ○ | identisch mit Agnitum Outpost 2.0 Pro | Virenscanner beigelegt | Remote-Verwaltung möglich |
| hilft zwar gegen Hacker-Attacken und Spyware, nicht gegen Trojaner | hilft zwar gegen Hacker- sowie einige Trojan- und Spy-Attacken, schlecht bedienbar | bekämpft zwar Hacks, aber kein Schutz gegen Trojaner und Spione | schützt wenig gegen Hacker, erstklassige Auswertung | schützt nur vor den wichtigsten Hacker-Angriffen | schützt vor Hackern, aber nicht vor Crackern und Spyware |

# Wertung & Ausstattung Software-Firewalls

| | | PLATZ 19 | PLATZ 20 | PLATZ 21 |
|---|---|---|---|---|
| **Produkt** | | **Zone Alarm 4.5 Pro** | **Personal Firewall 3.12** | **Firewall 4.05** |
| **Hersteller/Vertrieb** | | **Zonelabs (Vertrieb: S.A.D.)** | **Armor 2 Net** | **Mindsoft** |
| **Gesamturteil** | [Punkte] | **mangelhaft 40,4** | **mangelhaft 37,1** | **mangelhaft 23,2** |
| Leistung (75 %) | [Punkte] | 19. Platz 30,8 | 20. Platz 26,0 | 21. Platz 14,8 |
| Ausstattung (15 %) | [Punkte] | 9. Platz 72,0 | 7. Platz 74,0 | 24. Platz 48,7 |
| Bedienung (10 %) | [Punkte] | 11. Platz 64,8 | 11. Platz 64,8 | 23. Platz 48,2 |
| Info | | (073 05) 962 90 | customer@armor2net.com | info@mindsoft.es |
| Internet | | www.s-a-d.de | www.armor2net.com | www.mindsoft.es/english |
| Preis | | 50 Euro | 17 Euro | 20 Euro |
| kostenlose Version verfügbar | | ● | ○ | ○ |
| Einschränkungen kostenlose Version | | kein Packet-Level-Filter, eingeschränktes Auto-Detect | ○ | ○ |
| **Ausstattung** | | | | |
| Application Level Filter/ Packet Level Filter/Stateful Inspection | | ●/●/● | ●/●/● | ○/●/○ |
| Intrusion Detection (IDS)/ Stealth-Mode für Ports | | ●/● | ●/● | ●/● |
| Blockt Banner/Pop-ups/Flash-Ads | | ●/●/● | ○/●/○ | ○/○/○ |
| Blockt Skripte/ActiveX/Cookies | | ●/●/● | ○/○/○ | ○/○/○ |
| Autodetect Programme durch Hash-Wert/Autodetect Netzwerk | | ○/● | ○/● | ○/○ |
| Log nach Verbindung/Port/Programm/ filterbar/speicherbar | | ●/●/●/○/○ | ●/●/●/○/○ | ●/●/○/○/○ |
| Passwort-geschützt/Live-Update | | ●/○ | ●/● | ○/○ |
| Hotline | | (073 05) 96 29 30 | ○ | ○ |
| Sonstige Ausstattung | | ○ | Spyware-Scanner | ○ |
| Fazit | | wichtige Schwächen gegen Hacker, viele Trojaner und einige Spyware | simple Oberfläche, schwache Leistung | Tool mit vielen schwerwiegenden Bugs |

| | | PLATZ 22 | PLATZ 23 | PLATZ 24 |
|---|---|---|---|---|
| **Produkt** | | **Firekeys** | **Personal Firewall** | **Personal Firewall 2.0** |
| **Hersteller/Vertrieb** | | **Software Appliance** | **Surfsecret** | **Secure Up** |
| **Gesamturteil** | [Punkte] | **mangelhaft 20,4** | **mangelhaft 19,8** | **mangelhaft 16,5** |
| Leistung (75 %) | [Punkte] | 23. Platz 6,8 | 22. Platz 8,4 | 24. Platz 3,6 |
| Ausstattung (15 %) | [Punkte] | 15. Platz 63,3 | 17. Platz 57,3 | 16. Platz 59,3 |
| Bedienung (10 %) | [Punkte] | 13. Platz 58,0 | 22. Platz 48,8 | 21. Platz 49,1 |
| Info | | (+1) 95 22 53 84 00[1)] | support@surfsecret.com | (+1) 81 88 46 71 00[1)] |
| Internet | | softappco.com | www.surfsecret.com | www.secureup.com |
| Preis | | 34 Euro | 34 Euro | 25 Euro |
| kostenlose Version verfügbar | | ○ | ○ | ○ |
| Einschränkungen kostenlose Version | | ○ | ○ | ○ |
| **Ausstattung** | | | | |
| Application Level Filter/ Packet Level Filter/Stateful Inspection | | ○/●/○ | ○/●/○ | ○/●/○ |
| Intrusion Detection (IDS)/ Stealth-Mode für Ports | | ●/● | ●/● | ●/● |
| Blockt Banner/Pop-ups/Flash-Ads | | ○/●/○ | ○/○/○ | ●/●/○ |
| Blockt Skripte/ActiveX/Cookies | | ○/○/● | ○/○/○ | ○/○/○ |
| Autodetect Programme durch Hash-Wert/Autodetect Netzwerk | | ○/● | ●/○ | ○/○ |
| Log nach Verbindung/Port/Programm/ filterbar/speicherbar | | ●/●/●/●/● | ●/●/○/○/● | ○/○/○/○/○ |
| Passwort-geschützt/Live-Update | | ●/○ | ○/○ | ●/● |
| Hotline | | ○ | ○ | ○ |
| Sonstige Ausstattung | | ○ | ○ | ○ |
| Fazit | | wenig Schutz gegen die gefährlichsten Angriffsarten | zu simpel aufgebaut, viele s Sicherheitsleck | viele Sicherheitslücken und Programmfehler |

| | | Hersteller | Produkt |
|---|---|---|---|
| **Gesamturteil** | [Punkte] | | |
| Leistung (75 %) | [Punkte] | | |
| Ausstattung (15 %) | [Punkte] | | |
| Bedienung (10 %) | [Punkte] | | |
| Info | | | |
| Internet | | | |
| Preis | | | |
| **Ausstattung** | | | |
| DSL-Router/DSL-Modem/ ISDN-Router/ISDN-Modem | | | |
| Mitgelieferte Kabelarten | | | |
| Web-Interface | | | |
| DHCP vorhanden/aktiv | | | |
| NAT/Packet Filter/Stateful Inspection | | | |
| Anzahl WAN-Ports/LAN-Ports | | | |
| Angriffsprotokollierung | | | |
| DMZ einrichtbar/VPN möglich | | | |
| Garantie | | | |
| Hotline | | | |
| Fazit | | | |

| | | Hersteller | Produkt |
|---|---|---|---|
| **Gesamturteil** | [Punkte] | | |
| Leistung (75 %) | [Punkte] | | |
| Ausstattung (15 %) | [Punkte] | | |
| Bedienung (10 %) | [Punkte] | | |
| Info | | | |
| Internet | | | |
| Preis | | | |
| **Ausstattung** | | | |
| DSL-Router/DSL-Modem/ ISDN-Router/ISDN-Modem | | | |
| Mitgelieferte Kabelarten | | | |
| Web-Interface | | | |
| DHCP vorhanden/aktiv | | | |
| NAT/Packet Filter/Stateful Inspection | | | |
| Anzahl WAN-Ports/LAN-Ports | | | |
| Angriffsprotokollierung | | | |
| DMZ einrichtbar/VPN möglich | | | |
| Garantie | | | |
| Hotline | | | |
| Fazit | | | |

● = ja ○ = nein [1)] Auslandstarif

# Wertung & Ausstattung – Hardware-Firewalls

| | PLATZ 1 | PLATZ 2 | PLATZ 3 | PLATZ 4 | PLATZ 5 | PLATZ 6 |
|---|---|---|---|---|---|---|
| | **Zyxel** | **Netgear** | **3Com** | **Checkpoint** | **D-Link** | **Billion** |
| | **Zywall 2** | **FR 328 S** | **Cable/DSL Secure Gateway** | **Safe @ Office 105** | **DI-804 HV** | **Bipac 740 GE** |
| | gut 89,9 | gut 88,3 | gut 87,4 | gut 86,3 | gut 86,2 | gut 85,2 |
| | 1. Platz 93 | 4. Platz 91 | 4. Platz 91 | 4. Platz 91 | 1. Platz 93 | 4. Platz 91 |
| | 3. Platz 78 | 4. Platz 77 | 2. Platz 81 | 8. Platz 67 | 12. Platz 52 | 6. Platz 69 |
| | 4. Platz 84 | 3. Platz 85 | 9. Platz 70 | 6. Platz 80 | 2. Platz 86 | 11. Platz 66 |
| Support | (024 05) 690 90 | (08 00) 757 57 77[1] | (089) 25 00 00 | (08 11) 60 05 20 | (061 96) 779 90 | (040) 55 50 39 50 |
| Internet | www.zyxel.de | www.netgear-info.de | www.3com.de | www.checkpoint.de | www.dlink.de | www.billion-deutschland.de |
| Preis | 200 Euro | 250 Euro | 135 Euro | 300 Euro | 200 Euro | 150 Euro |
| | | | | | | |
| Schnittstellen | ●/●/○/○ | ●/○/○/○ | ●/○/○/○ | ●/○/○/○ | ●/○/○/○ | ●/●/○/○ |
| | 1 LAN, 1 WAN, 1 seriell für Konsole | 1 LAN | 1 LAN | 1 LAN | 1 LAN | 1 LAN, 1 DSL |
| Firewall | ● | ● | ● | ● | ● | ● |
| VPN | ●/● | ●/● | ●/● | ●/● | ●/● | ●/● |
| Management | ●/●/● | ●/●/● | ●/●/● | ●/●/● | ●/●/○ | ●/●/● |
| Durchsatz | 1/4 | 1/8 | 1/4 | 1/4 | 1/4 | 1/4 |
| Stateful Inspection | ● | ● | ● | ● | ● | ● |
| Content-Filter | ○/● | ○/○ | ●/● | ○/● | ○/● | ○/● |
| Garantie | 2 Jahre Bring-in-Garantie | 5 Jahre Bring-in-Garantie | 10 Jahre Bring-in-Garantie | 2 Jahre Bring-in-Garantie | 2 Jahre Bring-in-Garantie | 2 Jahre Bring-in-Garantie |
| Support | (018 05) 21 32 47[2] | (08 00) 757 57 77[1] | (018 05) 40 47 47[2] | (08 11) 60 05 20 | (08 00) 72 50 40 00[1] | (02 12) 22 67 18 50 |
| Fazit | Schnell und sicher, präzise Detailkonfiguration, mit DSL-Modem | sicher, schnellstes Gerät im Test, gut bedienbar | sicher, gut ausgestattet, einfach bedienbar und besonders preiswert | sicheres Gerät, gut bedienbar, aber sparsam ausgestattet | sicher und schnell, aber viel zu mager ausgestattet | sicheres Gerät inklusive DSL-Modem, Bedienung schwach |

| | PLATZ 7 | PLATZ 8 | PLATZ 9 | PLATZ 10 | PLATZ 11 | PLATZ 12 |
|---|---|---|---|---|---|---|
| | **Allnet** | **Bintec** | **Draytek** | **Linksys** | **SMC** | **Longshine** |
| | **ALL 1297 FW** | **Bingo DSL** | **Vigor 2600 X** | **BEFSX 41 DE** | **ADSL Barricade 7404 BRB** | **LCS-883R-DSL-2WN** |
| | gut 84,6 | befriedigend 75,9 | befriedigend 66,3 | befriedigend 65,9 | ausreichend 51,1 | mangelhaft 23,2 |
| | 3. Platz 92 | 8. Platz 86 | 10. Platz 59 | 9. Platz 63 | 11. Platz 43 | 12. Platz 9 |
| | 11. Platz 58 | 9. Platz 65 | 1. Platz 86 | 7. Platz 68 | 5. Platz 72 | 10. Platz 62 |
| | 10. Platz 69 | 12. Platz 16 | 1. Platz 91 | 4. Platz 84 | 6. Platz 80 | 8. Platz 71 |
| Support | (089) 89 42 22 22 | (09 11) 967 30 | (036 73) 86 64 34 | (018 03) 67 10 01[3] | (089) 92 86 10 | (041 02) 492 20 |
| Internet | www.allnet.de | www.bintec.de | www.draytek.de | www.linksys.de | www.smc.de | www.longshine.de |
| Preis | 330 Euro | 350 Euro | 270 Euro | 100 Euro | 160 Euro | 150 Euro |
| | | | | | | |
| Schnittstellen | ●/○/○/○ | ●/○/●/● | ●/●/●/● | ●/○/○/○ | ●/●/○/○ | ●/○/○/○ |
| | 1 LAN | 1 LAN, 1 ISDN 1Seriell für Konsole | 1 LAN, 1 DSL, 1 ISDN | 1 LAN | 1 LAN, 1 WAN | ○ |
| Firewall | ● | ○ | ● | ● | ● | ● |
| VPN | ●/● | ●/○ | ●/● | ●/● | ●/● | ●/● |
| Management | ●/●/○ | ●/●/● | ●/●/● | ●/●/● | ●/●/● | ●/●/● |
| Durchsatz | 1/4 und 1 ISDN | 1/1 | 1/4+1 ISDN | 1/4 | 1/4 | 2/4 |
| Stateful Inspection | ● | ● | ● | ● | ● | ● |
| Content-Filter | ●/● | ○/● | ○/● | ○/● | ●/○ | ○/○ |
| Garantie | 2 Jahre Bring-in-Garantie | 2 Jahre Bring-in-Garantie | 2 Jahre Bring-in-Garantie | 2 Jahre Bring-in-Garantie | 2 Jahre Bring-in-Garantie | 2 Jahre Bring-in-Garantie |
| Support | (089) 89 42 22 15 | (08 00) 73 33 73 33[1] | (036 73) 86 64 34 | (08 00) 101 33 11[1] | (08 00) 22 23 24 25[1] | (041 02) 49 22 23 |
| Fazit | Sicheres Gerät mit wenig Features, Bedienung sollte verbessert werden | Sicherheit noch gut, aber sehr schlecht bedienbar | Nur schwer gegen Angriffe abzudichten, ansonsten sehr leicht bedienbar | Sicherheitsmängel beim Bekämpfen von Hack-Attacken | schwere Konfigurations-mängel verhindern Sicherheit | veraltetes Gerät mit extremen Sicherheitsmängeln |

● = ja ○ = nein [1] gebührenfrei [2] 0,12 Euro pro Minute

# Spam-Abwehr

**Spam-Mails überfluten Firmen-Postfächer. E-Mail-Filter sollen die lästigen Nachrichten bereits zentral am Gateway erkennen und aussperren.**

Dirk Reichelt, Bertold Brackemeier

Mehr als die Hälfte aller E-Mails, die weltweit versendet werden, sind Spam-Mails. Genauer gesagt: rund 18 von 30 Milliarden Mails im Jahr 2003. Für den Mail-Empfänger sind die unverlangten Botschaften schlichtweg lästiger Datenmüll. Für Unternehmen sind Spam ein ernsthaftes Problem. Das Aussortieren und Löschen kostet Zeit und schadet damit der Produktivität der Mitarbeiter.

Doch der Netzwerk-Administrator kann die Mitarbeiter zumindest teilweise vor den lästigen Spams schützen. *PC Professionell* testet sieben aktuelle E-Mail-Filter für den Server: Clearswift Mailsweeper for SMTP 4.3, Cobion Orangebox Mail 2.0, Finjan Surfingate for E-Mail 7.0, Norman Spam Control 8, die »Empfehlung der Redaktion« Surfcontrol E-Mail-Filter for SMTP 4.7, Webwasher Spam Equator Prime 4.4. sowie Symantec Antivirus for SMTP Gateway 3.1. Die getesteten Programme ermöglichen das Filtern der Spam-Mails bereits am Gateway (Server), so dass im Idealfall kein Spam beim Mitarbeiter auftaucht. Mittels dieser zentralen Filter-Software lässt sich der ein- und ausgehende Mail-Verkehr überwachen. Die Filter von Clearswift, Cobion, Surfcontrol und Webwasher erkennen eingehende Spam-Mails nahezu gleich gut: Zwischen 90 und 92 Prozent liegt die Erkennungsrate. Im Mittelfeld bewegen sich die Programme von Finjan und Symantec mit Erkennungsraten um die 70 Prozent. Die rote Laterne hält das Norman-Produkt mit einer sehr niedrigen Rate unter 50 Prozent.

## Verwendete Filtertechniken

Eine der am häufigsten verwendeten Filtertechnologien ist der Zugriff auf Realtime-Blackhole-Lists, kurz RBLs. Darin sind bekannte E-Mail-Server verzeichnet, über die Spam verschickt wird. Noch präzisere Techniken verwenden Black-/Whitelists für Keywords und Adressen für Absender, Empfänger, Betreff und Mail-Nachricht, um potenziellen Spam aufzuspüren. Die Listen lassen sich in der Regel entweder per Hand erweitern oder aber automatisch via Internet wie bei Surfcontrol. Die Hersteller Cobion, Webwasher, Clearswift und Surfcontrol setzen auf einen Datenbank-gestützten Filter. Der Test

## Empfehlungen der Redaktion

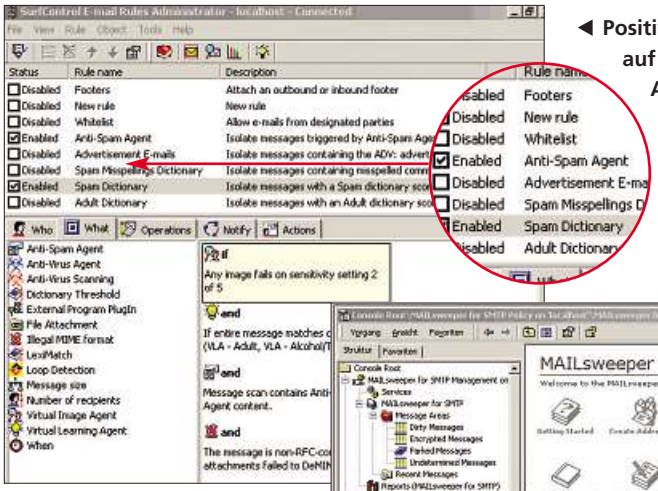
**Surfcontrol E-Mail-Filter for SMTP 4.7**
Die beste Erkennungsleistung liefert Surfcontrol. Weitere Stärken des Produkts sind die einfache Bedienung und umfassende Ausstattung. Der Anwender findet neben einfachen Analysetools auch einen trainierbaren Filter.

**Webwasher Spam Equator 4.4**
Einen gut konfigurierbaren E-Mail-Filter mit vielen Einstellmöglichkeiten bietet Webwasher. Der Preis von 625 Euro überzeugt zudem und macht Spam Equator zum Budget-Sieger.

| | Produkt Hersteller | (maximal 100 Punkte) |
|---|---|---|
| 1 | **E-Mail-Filter for SMTP 4.7** Surfcontrol | 89,4 |
| 2 | **Mailsweeper for SMTP 4.3** Clearswift | 87,3 |
| 3 | **Spam Equator Prime 4.4** Webwasher | 86,4 |
| 4 | **Orangebox Mail 2.0** Cobion | 84,5 |
| 5 | **Surfingate for E-Mail 7.0** Finjan | 76,5 |

zeigt, dass diese Methode deutlich erfolgreicher ist. Die Software gleicht die Mails mit der Datenbank bekannter Spams ab und berücksichtigt dabei auch im Mail-Text eingebaute Bilder und URLs. Auf diese Weise teilt der Filter die Nachrichten in unterschiedliche Kategorien ein und ermöglicht so ein detailliertes Aussperren unerwünschter Nachrichten. Die Aktualisierung und Pflege der Datenbank kann der Administrator per Hand vornehmen. Zeitsparender und bequemer ist allerdings ein Auto-Update, wie bei Surfcontrol.

Sämtliche Mail-Filter auf dem *PC-Professionell*-Prüfstand sind als SMTP-Relay in der Lage, E-Mail-Nachrichten aus dem Internet entgegenzunehmen und diese nach der Analyse an die internen Mailserver des Unternehmens weiterzuleiten. Damit erkennen die Kandidaten nicht nur eingehende Spams, sondern kontrollieren zusätzlich alle ausgehenden Botschaften. Der Security-Administrator kann somit auch den Versand vertraulicher Informationen und Dokumente unterbinden.




◀ **Positiv: Surfcontrol setzt auf unterschiedliche Analyse-Werkzeuge bei der Identifizierung von Spam-Mails.**

▶ **Das Filtern der Nachrichten erfolgt bei Clearswift auf mehreren Wegen.**

## Surfcontrol E-Mail-Filter for SMTP 4.7

Gelungen und überzeugend ist das Basis-Setup des Filters. Hierbei werden alle Einstellungen für die Mail-Verteilung abgefragt und verfügbare Updates aus dem Internet geladen. Das bietet sonst nur Symantec. Die Steuerung des Filters erfolgt per Webbrowser oder Windows-Software. Die Filterregeln werden aus Objekten der Kategorien Who, What, Operation, Notify und Action zusammengesetzt. So lassen sich aus einer umfangreichen Vorauswahl mit wenigen Klicks präzise Regeln konfigurieren. Das ist sehr einfach für den Administrator und besser gelöst als bei den anderen Testkandidaten.

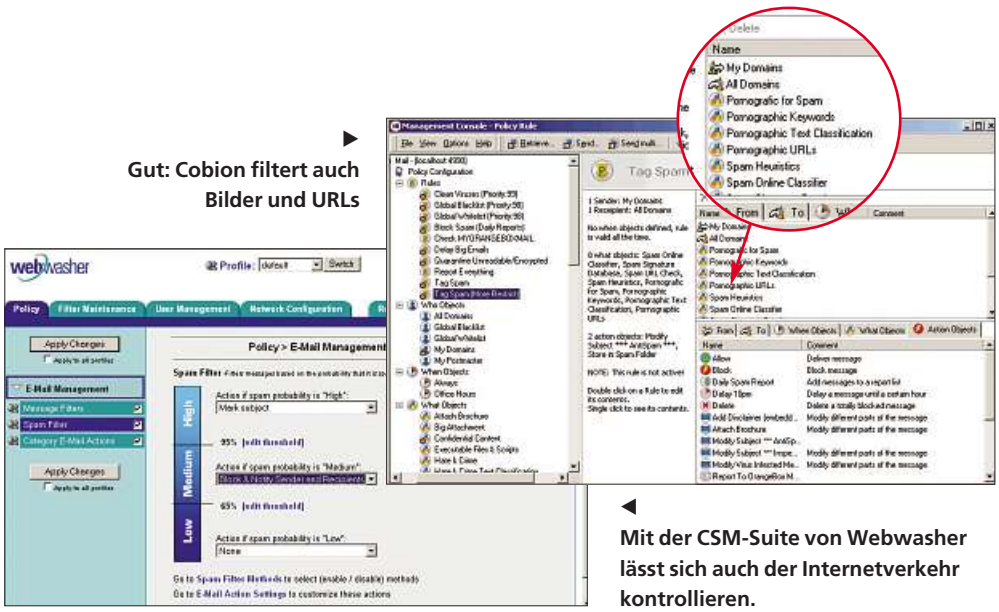
Durch die Kombination von RBLs und Blacklists, intelligentem Spam-Filter und Image-Analyse (via Bilddatenbank) erzielt ein E-Mail-Filter for SMTP die besten Testergebnisse bei der Spam-Analyse. Die Spam-Erkennungsrate beträgt 91,9 Punkte – ein sehr guter Wert. Für die Erkennung der Nachrichten besteht die Möglichkeit, diese zu modifizieren, zu blockieren oder zu verzögern. Zusätzlich ist ein Surfcontrol-Virenscanner integriert. Die Installation der Software erfordert einen Windows-Server sowie eine MSDE-Datenbank. Probleme bereitet die Datenbankanbindung während des Installationsprozesses. Sowohl mit einem vorbereiteten SQL-Server als auch mit der installierten MSDE ist die Zusammenarbeit nur möglich, wenn für den User kein Passwort gesetzt ist.

Die Surfcontrol-Software überzeugt durch einfache Bedienung und sehr guter Ausstattung. Dank umfangreicher Analyse-Tools werden die Testnachrichten am zuverlässigsten gefiltert. Das verdient die »Empfehlung der Redaktion«. 25 User-Lizenzen kosten 1575 Euro.

## Clearswift Mailsweeper for SMTP 4.3

Als einziger Testkandidat beginnt der Clearswift-Filter erst mit der Installation, wenn der Anwender die Endung der zu überwachenden Toplevel-Domain eingetragen hat. Nach der Korrektur dieses Fehlers verläuft die initiale Installation reibungslos. Bereits bei der Installation wird das komplette Basis-Setup des Filters bestimmt. Dieser ist sofort einsatzfähig. Die Administration der Software erfolgt mit einem Snap-in für die Microsoft-Management-Konsole. Ebenfalls einzigartig im Test: Mailsweeper bietet die Möglichkeit, die Gewichtung für die Einträge im Wörterbuch selbst anzupassen, und ermöglicht damit eine detaillierte Konfiguration des Filters. Ingesamt gehört Clearswift bei der Spam-Erkennung mit einer Erkennungsrate von 89,4 Punkten zu den Besten im Testfeld. Für zusätzlichen Schutz vor Viren lassen sich gängige Virenscanner über eine Schnittstelle einbinden.

Mailsweeper bietet umfangreiche Funktionen zur Kontrolle von ein- und ausgehenden Mails. Ein Pluspunkt des 1841 Euro teuren Produkts ist die sehr gute Assistenten-Unterstützung. Den ersten Platz verspielt Clearswift nur wegen der gegenüber dem Testsieger niedrigeren Spam-Erkennung.




▶ **Gut: Cobion filtert auch Bilder und URLs**

◀ **Mit der CSM-Suite von Webwasher lässt sich auch der Internetverkehr kontrollieren.**

## Webwasher Spam Equator Prime 4.4

Ohne Probleme verläuft die Installation von Spam Equator Prime. Da der Mail-Filter Bestandteil der CSM-Suite (Content Security Management) von Webwasher ist, muss zunächst das komplette Software-Paket installiert werden. Erst der Lizenz-Key entscheidet, welche Funktionen nutzbar sind. Der Netzwerk-Administrator zahlt lediglich für die Features, die er wirklich nutzt. Die komplette Administration des E-Mail-Filters erfolgt mittels Web-Frontend. Dieses lässt sich direkt auf dem Server oder über das LAN aufrufen. Wegen der vielfältigen Einstellungsmöglichkeiten sind einige Stunden Einarbeitungszeit für den richtigen Umgang mit dem Web-Frontend notwendig. Mit einem Acht-Schritte-Assistenten nimmt der Administrator in wenigen Minuten die grundlegenden Einstellungen für Relay-Hosts, RBL-Server sowie den Mail-Filter vor. Für die Filterung setzt Webwasher neben dem Abgleich mit RBLs, Keywords und Black-/Whitelists einen intelligenten Filter ein, der die Spam-Wahrscheinlichkeit für eine Nachricht errechnet. Mit 89,8 Punkten Erkennungsrate erreicht Spam Equator Prime die zweitbeste Leistung.

Für die Verarbeitung der Nachrichten stehen vielfältige Optionen vom Blockieren über Verzögern bis hin zur Kennzeichnung der Mail für den Empfänger zur Verfügung. Über eine Schnittstelle lässt sich ein Virenscanner in den Filterprozess einbinden.

Webwasher bietet einen intelligenten Mail-Filter, mit dem die Einstufung und Verarbeitung unerwünschter Nachrichten sehr gut steuerbar ist. Selbst der Preis von 625 Euro für 25 Lizenzen überzeugt im Vergleich. Webwasher erhält infolgedessen die »Budget-Empfehlung« von *PC Professionell*.

## Cobion Orangebox Mail 2.0

Die Installation des E-Mail-Filters von Cobion setzt voraus, dass Microsofts XML-Paket (Version 4.0) sowie Office (ab Version 2000) und Outlook installiert sind. Negativ ist, dass bei der Installation des Filters die für die Administration notwendige Windows-Anwendung nicht automatisch installiert wird. Die Administration mit dem Windows-Tool erfolgt entweder auf dem lokalen System oder über das LAN. Beim ersten Start ist zunächst das zu verwendende SMTP-Gateway anzugeben. Orangebox unterstützt dabei nicht die Möglichkeit, die gescannten Nachrichten direkt an einen lokal installierten Mailserver weiterzuleiten, die Mails bleiben auf dem Server. Eine Filterregel wird mit wenigen Klicks aus den Bereichen Who, When, What und Action zusammengesetzt. Für die Spam-Analyse greift der Filter auf eine Datenbank sowie individuell zu pflegende Keyword-Listen zurück. Die Erkennungsrate liegt bei 90,4 Punkten, ein hervorragender Wert im Vergleichstest. Nachteilig ist jedoch, dass keine Möglichkeit besteht, in die Wahrscheinlichkeitsbewertung der eingehenden Mails einzugreifen. Über eine Schnittstelle lassen sich Virenscanner von McAfee, Sophos oder Symantec einbinden.

Orangebox Mail zeigt im Test gute Ergebnisse. Ein intuitiv zu bedienendes Administrations-Frontend erlaubt einfachen Umgang mit dem Filter. Allerdings sind 1190 Euro (25 User, 1 Jahr Updates) im Vergleich beispielsweise zu Webwasher zu teuer.

## Finjan Surfingate for E-Mail 7.0

Vor der Installation des E-Mail-Filters muss die Finjan-eigene Datenbank installiert sein. Filter-Software, Datenbank und Administra-

tor-Frontend können dabei auf unterschiedlichen Systemen laufen. Dass dies durchaus ratsam ist, zeigt die Auslastung des Testsystems. Bereits bei einem minimalen Datenaufkommen belegen Datenbank und Filter-Software 270 MByte.

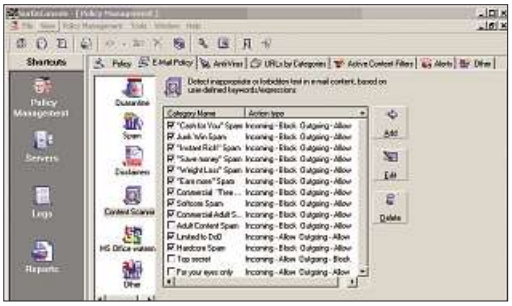
Umständlich ist, dass auf dem Windows-Server zur Installation der Internet Information Server (IIS) mit SMTP-Dienst oder ein Exchange Server vorhanden sein muss. Sämtliche Einstellungen werden per Windows-Frontend vorgenommen. Praktisch: Bei der Spam-Erkennung sind bereits einige RBLs vorkonfiguriert. Für eine schnelle Administrator-Auswertung der Spam-Mails speichert der Filter die letzten RBL-Anfragen zwischen.

Als einziger Hersteller stattet Finjan seine Software neben dem obligatorischen englischen Wörterbuch mit einer deutschen Wörterliste aus. Diese ist allerdings unzureichend, so dass bei deren Einsatz lediglich eine einzige zusätzliche deutschsprachige Spam-Mail erkannt wird. Integriert ist zudem ein Virenscanner von McAfee.

Filteraufgaben erfüllt die Finjan-Software mit der Erkennungsrate von 71,9 Punkten nicht überzeugend. Zudem sollte aufgrund der hohen Ressourcen-Anforderungen Finjan auf einem dedizierten System installiert werden. Hersteller wie Surfcontrol oder Clearswift erlauben komfortableres Arbeiten. Das Programm ist mit 3100 Euro das teuerste im Vergleichstest von *PC Professionell*, unterstützt dafür jedoch 100 User.

### Symantec Antivirus for SMTP Gateway 3.1

Ohne Probleme verläuft die Installation, nach deren Abschluss wird automatisch ein Update der Signaturdatenbanken ausgeführt. Die Steuerung des Filters erfolgt schnell und übersichtlich per Webbrowser. Für die Filterung der E-Mail-Nachrichten lassen sich eigene Black-/Whitelists für Absender, Empfänger und Betreff pflegen. Zusätzlich kann der Filter mit einem heuristischen Verfahren Spam erkennen und eine Spam-Wahrscheinlichkeit ermitteln. Mittels dieser Technik erkennt die Symantec-Software als einziger Filter im Test neben Surfingate auch deutsche Spams. Gleichzeitig stuft der Filter als Einziger jedoch eine korrekte Nachricht fälschlich als Spam ein. Die Erkennungsrate liegt im unteren Testfeld: 70,8 Punkte. Der Netzwerk-Administrator kann nicht selbst Einfluss auf die Einstufung der Mails nehmen. Nützliche Infos wie die Spam-Wahrscheinlichkeit für eine Mail finden sich nur bei der Logfiles-Auswertung.



▲ **Gut: Finjan setzt bei der E-Mail-Filterung auf eine eigene Datenbank.**

Der SMTP-Filter bietet guten Schutz vor Viren und Spam. Jedoch fehlt es an Optionen zur Optimierung. So bleibt die Filterleistung dem Mitbewerb unterlegen. Der Preis ist mit 408 Euro für 25 User angemessen.

### Norman Spam Control 8.0

Norman Spam Control setzt die Installation eines Microsoft Exchange Servers oder des Internet Information Server (IIS) voraus. Ohne Probleme integriert sich der Filter in den SMTP-Dienst von IIS im Testsystem und ist sofort nach der Installation einsatzbereit. Die Steuerung des Filters erfolgt bequem mittels eines Snap-ins für die Microsoft-Management-Konsole. Für das Filtern setzt Norman auf RBLs und Keywords. Dabei stellt der Hersteller eine vorkonfigurierte englische Wörterliste zur Verfügung. Hierfür besteht aber nur die Möglichkeit, die Mails auf dem Server zu verschieben, zu löschen oder an einen speziellen E-Mail-Account weiterzuleiten.

Im Test liegt die Erkennungsrate bei 41,8 Punkten, das ist zu wenig. Als spezielles Blocking-Feature bietet der Filter die Möglichkeit, per Blacklist zu bestimmen, welche Sprachen in einer E-Mail gestattet sind. Das Monitoring-Tool sowie die verfügbaren Reportfunktionen für Überwachung und Auswertung beschränken sich nur auf die notwendigsten Angaben.

In Sachen Ausstattung hat Spam Control starke Defizite. Hier fehlt es an individuellen Filtern sowie einer Datenbank-gestützten Mail-Analyse. Das Tool kostet 311 Euro für 25 User, ist aber trotz des günstigen Preises nicht zu empfehlen. BBR

## Alternative Open Source

Wer Spam wirksam bekämpfen will, ohne viel Geld auszugeben, findet in dem kostenlosen Anti-Spam-Tool Spam Assassin *(spamassin.org)* eine gute Software, die bereits in vielen Unternehmen eingesetzt wird. Das Programm bietet maximale Erkennungsraten von 95 Prozent. In Bedienkomfort und Zusatzfunktionalität heben sich die getesteten Spam-Filter aber deutlich von Spam Assassin ab. Dem Tool fehlt etwa eine gängige Web-Oberfläche zur Administration.

# Wertung & Ausstattung

| | PLATZ ① | PLATZ ② | PLATZ ③ | PLATZ ④ |
|---|---|---|---|---|
| | PC PROFESSIONELL Empfehlung der Redaktion | | PC PROFESSIONELL Budget Empfehlung | |
| | SurfControl |  | webwasher |  |
| **Produkt** | **E-Mail-Filter for SMTP 4.7** | **Mailsweeper for SMTP 4.3** | **Spam Equator Prime 4.4** | **Orangebox Mail 2.0** |
| **Hersteller** | **Surfcontrol** | **Clearswifft** | **Webwasher** | **Cobion** |
| **Gesamturteil** [Punkte] | **gut 89,4** | **gut 87,3** | **gut 86,4** | **gut 84,5** |
| Spam-Erkennung (60 %) [Punkte] | 1. Platz 91,9 | 4. Platz 89,4 | 3. Platz 89,8 | 2. Platz 90,4 |
| Usability (25 %) [Punkte] | 1. Platz 84,0 | 3. Platz 81,5 | 2. Platz 82,0 | 5. Platz 75,0 |
| Service (15 %) [Punkte] | 2. Platz 88,3 | 2. Platz 88,3 | 6. Platz 80,0 | 7. Platz 76,7 |
| Info | (+44) 12 60 29 62 53[1] | (040) 23 99 90 | (052 51) 50 05 40 | (05 61) 57 08 70 |
| Internet | www.surfcontrol.com | www.clearswift.de | www.webwasher.de | www.cobion.de |
| Preis | 1575 Euro, 25 User[2] | 1841 Euro, 50 User[2] | 625 Euro, 25 User[2] | 1190 Euro, 25 User[2] |
| **Filterliste/Filter** | | | | |
| Subject/Absender/Keywords | ●/●/● | ●/●/● | ●/●/● | ●/●/● |
| Black-/Whitelist pflegbar | ● | ● | ○ | ● |
| Kategoriebezogene Mail-Filterung | ● | ● | ● | ● |
| RBL-Unterstützung | ● | ● | ● | ● |
| Mailgröße/Anzahl begrenzen | ●/● | ●/● | ●/● | ●/● |
| Schnittstelle Virenscanner | ● | ● | ● | ● |
| Intelligenter Filter/konfigurierbar | ●/● | ●/● | ●/● | ●/○ |
| Mail blockieren/verzögern | ●/● | ●/● | ●/● | ●/● |
| Benachrichtigung Absender/ Empfänger/Postmaster | ●/●/● | ●/●/● | ●/●/● | ●/●/● |
| **Service** | | | | |
| Handbücher | Englisch | Englisch | Englisch | Englisch |
| Hotline | (+44) 12 60 29 62 53[1] | (040) 23 99 90 | (052 51) 50 05 40 | (05 61) 57 08 72 77 |
| Fazit | guter Mail-Filter, hervorragende Filter, beste Spam-Erkennungsrate im Test | sehr gute Anwender-Unterstützung via Assistenten, gute Spam-Erkennung | intelligente, hervorragende Filter, gute Spam-Erkennung, gelungene Web-Oberfläche | intuitive Bedienung, einfaches Handling, noch gute Erkennungsrate |

| | PLATZ ⑤ | PLATZ ⑥ | PLATZ ⑦ |
|---|---|---|---|
| | finjan. software |  |  |
| **Produkt** | **Surfingate for E-Mail 7.0** | **Antivirus for SMTP** | **Spam Control 8.0** |
| **Hersteller** | **Finjan** | **Symantec** | **Norman** |
| **Gesamturteil** [Punkte] | **befriedigend 76,5** | **befriedigend 71,3** | **ausreichend 52,3** |
| Spam-Erkennung (60 %) [Punkte] | 5. Platz 71,9 | 6. Platz 70,8 | 7. Platz 41,8 |
| Usability (25 %) [Punkte] | 4. Platz 79,5 | 6. Platz 62,0 | 7. Platz 58,0 |
| Service (15 %) [Punkte] | 1. Platz 90,0 | 2. Platz 88,3 | 5. Platz 85,0 |
| Info | (081 02) 89 78 28 | (021 02) 745 30 | (02 12) 26 71 80 |
| Internet | www.finjan.com | www.symantec.de | www.norman.de |
| Preis | 3100 Euro, 100 User[2] | 408 Euro, 25 User | 311 Euro, 25 User |
| **Filterliste/Filter** | | | |
| Subject/Absender/Keywords | ●/●/● | ●/●/● | ●/●/● |
| Black-/Whitelist pflegbar | ● | ● | ○ |
| Kategoriebezogene Mail-Filterung | ● | ○ | ● |
| RBL-Unterstützung | ● | ● | ● |
| Mailgröße/Anzahl begrenzen | ●/● | ●/● | ○/● |
| Schnittstelle Virenscanner | ● | integriert | ○ |
| Intelligenter Filter/konfigurierbar | ○/○ | ●/○ | ○/○ |
| Mail blockieren/verzögern | ●/○ | ●/○ | ●/○ |
| Benachrichtigung Absender/ Empfänger/Postmaster | ○/○/○ | ●/○/● | ○/○/● |
| **Service** | | | |
| Handbücher | Englisch | Englisch | Englisch |
| Hotline | (081 02) 89 78 28 | (021 02) 745 30 | (01 90) 87 22 36[3] |
| Fazit | zu hohe Ressourcenanforderung an den Server, befriedigende Erkennungsraten | guter Schutz vor Viren und Spam, befriedigende Filter, kein Finetuning möglich | schlechte Spam-Erkennung, Defizite bei der Ausstattung, keine individuellen Filter |

● = ja ○ = nein [1]Auslandstarif [2]inklusive 1 Jahr kostenloses Update [3]1,86 Euro/Min

## Glossar

**Blacklist** Ausschlussliste für Spam-Mails. Hier werden Spam-Absender gesammelt und mit den Absendern eingehender Mails abgeglichen. Bei einer Übereinstimmung werden die Spam-Mails herausgefiltert.

**Heuristik** Heuristiken analysieren alle ausführbaren Programme nach viren- und spamrelevanten Merkmalen. Dabei werden bestimmte Sequenzen in Assembler-Befehle übersetzt.

**Open-Relay** Server, die alle Mail-Anfragen akzeptieren und an jede Domain ausliefern.

**RBL** Realtime-Blackhole-List. Hier werden E-Mail-Server verzeichnet, von denen bekannt ist, dass über sie Spam-Nachrichten verschickt werden.




# Praxis

Windows ist von Haus aus unsicher und bietet Hackern viele Angriffspunkte. Erst mit erweiterten Einstellungen und einigen Zusatzprogrammen lassen sich Sicherheitslücken schließen. *PC Professionell* zeigt in ausführlichen Anleitungen, was Anwender beachten müssen und wie sie zukünftig sicher im Web unterwegs sein können.

## INHALT

76 **System-Spitzel**
82 **Online-Checks**
84 **XP-Sicherheit**
87 **Windows-98-Schutz**
90 **Abhörsicher**
93 **Linux-Spam-Filter**

# System-Spitzel

**Profihacker haben es auf Firmennetze abgesehen, doch auch private User sind in Gefahr. Korrekte Systemeinstellungen, Firewalls und Netz-Tools wehren Attacken ab.**

Oliver Ibelshäuser

Bevorzugte Angriffsziele von Hackern sind Webserver. Aus Unternehmenssicht rückt daher auch das Webprotokoll HTTP in den Blickpunkt. Hintergrund: HTTP nutzt den Port 80, den jede Firewall freigibt, damit der Anwender überhaupt surfen kann. Folglich dient der Port 80 auch für Hacker als Schleuse ins System. Die Möglichkeiten der Zugriffe reichen vom Buffer-Overflow über Cross-Site-Scripting bis zum Ausführen bösartiger Perl-Kommandos (Perl-Shell) auf manipulierten Seiten.

Endanwender sind von diesem Problem ebenfalls betroffen, wenn auch in geringerem Maße. Für den User, der per Einwählverbindung ins Internet geht, gerät der eigene PC statt des Firmen-Webservers ins Fadenkreuz.

Einen gewissen Teil der Gefahren bannen Security-Patches für Browser und Betriebssystem. Microsoft veröffentlicht etwa regelmäßig Sicherheits-Updates, die vor allem die Gefahr eines Buffer-Overflow-Angriffs bannen. Firewalls lassen die Pakete in der Regel passieren, sofern nicht per Definition nur unbedenkliche Seiten geladen werden können.




▲ **In unvernetzten Umgebungen ist die Datei- und Druckerfreigabe für Microsoft-Netze ein Sicherheitsrisiko.**

## Privatanwender im Fadenkreuz

Für private Anwender ist die Gefahr, Opfer einer Attacke zu werden, ähnlich groß wie für Firmen. Allerdings sehen sich die Endanwender anderen Bedrohungen ausgesetzt. Das Lahmlegen von Servern mit Hilfe von Buffer-Overflow-Attacken haben Heimanwender nicht zu fürchten. Stattdessen drohen Datensabotage und -diebstahl. Als Hilfsmittel dienen dazu Trojanische Pferde und Backdoor-Viren. Vor allem Filesharing-Foren wie Kazaa haben sich als Malware-Schleudern etabliert. Neben dem gewünschten MPEG-File lädt sich der Besucher beispielsweise noch unwissentlich den Server eines Trojaners. Bei populären Backdoor-Programmen sind diese Server-Tools nur wenige hundert KByte groß und lassen sich recht gut in größeren Dateien verstecken. Tückisch: Moderne Varianten von Back Orifice oder Subseven laufen im Stealth-Modus und verbrauchen kaum Ressourcen, so dass die Spionage mitunter lange unentdeckt bleibt.

## 500 KByte kleine Spione

Trojaner-Angriffe sind deshalb recht häufig, weil der Angreifer praktisch keinerlei Hacker-Know-how benötigt. Back Orifice und Netbus

**Ein Sniffer registriert die Datenanfragen eines Hackers über verschiedene Ports. ▶**

| | | | | | | |
|---|---|---|---|---|---|---|
| PC-PRO | [redacted] | 14 | 14 | Out | 0 | 137 |
| PC-PRO | [redacted] | 144 | 159 | Out | 14 | 139,137,20034 |
| PC-PRO | [redacted] | 74 | 87 | In | 13 | 5000,139,138,3000,3033,1098,1967,1968,1969,1970,1971 |
| PC-PRO | [redacted] | 4 | 4 | Out | 0 | 20034,137 |
| PC-PRO | [redacted] | 3 | 3 | Out | 0 | 138 |
| PC-PRO | [redacted] | 3 | 3 | Out | 0 | 138 |




**▲ Blendet der Anwender die regulären Microsoft-Dienste aus, zeigt die Liste nur noch Prozesse von anderen Herstellern.**

helfen selbst bei der Installation mit komfortablen Assistenten. Aufgrund dieser simplen Handhabung der Tools fallen Trojaner-Täter in die Klasse der Skript-Kiddies. Auch Viren-Boten zählen dazu, die etwa vorhandene VB-Skripts nur geringfügig abändern und weiterverschicken. Trojaner gliedern sich in zwei Komponenten: den Server und den Client. Das Server-Tool wird beim Opfer installiert, liefert die gewünschten Daten und führt dort lokal Remote-Befehle aus. Der Angreifer hat auf dem Rechner die gleichen Rechte wie das Opfer selbst – wiederum ein Argument dafür, in Windows XP grundsätzlich nur mit einem eingeschränkten Benutzerkonto zu surfen. Für den Hacker stellt sich nur das Problem, den Server unbemerkt auf dem PC des Opfers zu installieren. Das gelingt, indem die selten mehr als 500 KByte fassenden Sende-Programme heimlich aufgespielt oder aber als Attachment per Mail versendet werden. Dann allerdings muss das Server-Tool vorkonfiguriert werden, so dass die Anwendung als versteckter Task mitläuft und bei jedem Windows-Start automatisch aufgerufen wird.

Perfide: Der Hacker gibt dem Server auf Wunsch ein Passwort mit, so dass nur er für den verbotenen Zugriff exklusive Rechte besitzt. Ist kein Passwort gesetzt, kann jeder Angreifer mit dem passenden Client den PC des Opfers attackieren.

## Anatomie eines Angriffs

Ist der Server beim Opfer platziert, kann der Hacker die Verbindung aufnehmen. Dafür gibt es zwei Möglichkeiten. Falls der Angreifer zum Beispiel sein Gegenüber kennt, muss er lediglich die IP-Adresse des Rechners ermitteln. Komfortabler erfolgt der Zugriff allerdings, wenn der Hacker den Trojaner selbst damit beauftragt, die IP-Adressen möglicher Angriffsziele ausfindig zu machen. Netbus hat dafür beispielsweise eine komfortable Maske und scannt den kompletten Bereich zwischen zwei IP-Adressen im Web. Alle Treffer listet das Tool in einer Box auf. Allerdings verlangt Netbus die Eingabe eines Ports auf dem Zielrechner für den Zugriff. Über diesen offenen Port läuft im Anschluss die komplette Datenkommunikation. Gute Chancen hat der Angreifer, wenn er auf einen Netbios-Port zurückgreift, etwa 138 oder 139, da diese Ports für Drucker und gemeinsame Dokumente per Default geöffnet sind. Andernfalls hilft nur das Ausprobieren weiterer Ports. Immerhin ist die Auswahl mit weit über 65 000 Schleusen ins System groß genug.

Über die Funktion Connect oder Connect Server beginnt der Host den verbotenen Zugriff. Zwar findet Netbus über den IP-Scan alle Rechner in einer bestimmten IP-Range mit geöffnetem Port, der Kontakt mit dem Netbus-Server gelingt aber nur, wenn die TCP-Anfrage nicht von einer Firewall abgewiesen wird. Übrigens: Während Netbus lediglich über TCP/IP kommuniziert, was deutlich unauffälliger und sicherer ist, lässt beispielsweise Back Orifice dem Angreifer die Wahl, auch UPD-Pakete zu senden.

Läuft der Server nicht im Tarnmodus, zeigt dieser die IP-Adresse des Angreifers im Hauptfenster an. Von nun an hat der Hacker alle Rechte auf dem Remote-PC, die der lokale Nutzer auch besitzt. So lassen sich Files einsehen, löschen, neu anlegen, die Windows-Konfiguration ändern oder Passwörter erspähen. Als zusätzliche Störfunktionen gestattet Netbus beispielsweise auch, auf dem Opfer-PC die CD-Lade ein- und auszufahren, die Tastatur zu blockieren oder die Maustasten zu vertauschen.

## Trojaner entlarven

Auch der beste Stealth-Modus eines Backdoor-Programms verhindert nicht, dass eindeutige Spuren im System auf die Malware hinweisen. Beim Verdacht eines Angriffs ist die Registry stets die erste Anlaufstelle. Programme, die standardmäßig bei jedem Windows-Start geladen werden, liegen unter Windows XP und Windows 2000 im Schlüssel *Hkey_Local_Machine/Software/Microsoft/Windows/CurrentVersion/Run*. Allerdings wählen die Trojaner unverfängliche Dateinamen, etwa *patch.exe* bei Netbus. Der Parameter *nomsg* (no message) ist ein klarer Hinweis auf eine heimliche Anwendung.

Auch der Taskmanager entlarvt den Spion. Netbus 2.0 beispielsweise startet einen Prozess namens *nbsvr.exe*. Der Server von Back




▲ **Die Sicherheits-Software Hacker-Eliminator listet alle Prozesse auf, die aktuell Kontakt zum Internet herstellen.**

Orifice 2000 heißt *bo2k.exe*, der von Subseven *server.exe*. Tückisch: Nach der Konfiguration des Servers (IP-Adresse, Port, Mail-Adresse für Key-Logs) wird ganz sicher jeder versierte Hacker die Bezeichnung der Datei in einen unverfänglichen Namen ändern.

Auch das Systemkonfigurationsprogramm gewährt hilfreiche Einblicke in laufende und automatisch gestartete Dienste und Anwendungen. Der schnellste Weg dorthin führt über die Ausführen-Box und den Befehl *msconfig -6*. Der Zusatz *-6* startet direkt die gewünschte Registerkarte *Systemstart*. In der folgenden Liste führt Windows alle automatisch gestarteten Dienste auf und bildet damit die Registry ab. Neben dem Reg-Pfad steht der originäre Dateipfad zur Anwendung, was die Diagnose der Malware erleichtert. Wer das Häkchen vor dem jeweiligen Eintrag löscht, deaktiviert das Programm dauerhaft bei künftigen Systemstarts.

Als sinnvoll erweist sich ebenfalls ein Blick in die laufenden Services im Register Dienste. Windows katalogisiert hier sämtliche automatisch gestarteten Dienste. Die Liste ist jedoch nicht identisch mit den Aufzählungen im Taskmanager, der die Services regelmäßig aktualisiert. Mit einem Haken vor dem Eintrag *Alle Microsoft Dienste ausblenden* sorgt der Anwender für mehr Übersicht.

## Profi-Tool: Hacker-Eliminator

Mit der kostenlosen Demoversion von Hacker-Eliminator spart sich der Anwender die Suche in den Windows-Diensten und verdächtigen Einträgen in der Registry. Das Programm ist einfach zu bedienen und listet geheime Services, versteckte File-Extensions und offene Ports auf. Praktisch: Jeder neu gestartete Dienst veranlasst das Tool sofort zu einer Dialog-Abfrage, ob der Anwender die Datei zulassen oder stoppen möchte. Eine History der laufenden Prozesse gewährt zudem tiefe Einblicke in Systemvorgänge.

Um mögliche Online-Attacken zu erkennen, listet das Tool unter *Servers* im Bereich *Tools* alle Dienste und Programme auf, die eine aktive Anbindung ans Internet besitzen. Anhand des zugehörigen Dateipfades lässt sich leicht ausmachen, ob es sich um eine unerwünschte Verbindung handelt.

Abgerundet wird dieser Sicherheitsdienst von sinnvollen Internet-Funktionen wie Whois, die zu einer IP-Adresse den zugehörigen Server ermittelt, und Trace-Route, die den Weg eines möglichen Angreifers zurückverfolgt. Eine auf 30 Tage befristete Version von Hacker-Eliminator ist kostenlos erhältlich *(hacker-eliminator.com)*. Die Einjahreslizenz kostet 99 Dollar.

## Malware ausschalten

Die bislang vorgestellten Methoden ermitteln vor allem bösartige Dateien auf dem Rechner. Doch diese kostenlosen Tools und Bordmittel leisten noch mehr: So lässt sich damit nachvollziehen, wer der Angreifer ist, wann dieser Kontakt aufnimmt und welche Daten gestohlen werden. Um mögliche Angriffe überhaupt auszumachen, muss der Anwender potenzielle Ziele auf dem eigenen Rechner kennen. Von großer Bedeutung ist hier die eigene IP-Adresse. Der User ermittelt die Zahlenkolonne über die Netzwerk-Verbindungen in der Systemsteuerung. Ein Klick auf die Eigenschaften im Dialog *Eigenschaften von LAN-Verbindung* gibt die bis zu zwölfstellige Kombination frei, wenn der Benutzer den Eintrag Internetprotokoll (TCP/IP) im Fenster *Diese Verbindung verwendet folgende Elemente* aktiviert. Internet-Anwender, die sich über einen Provider wie T-Online oder Freenet ins Internet einwählen, haben eine dynamische IP-Adresse. Diese wird nach jeder Einwahl vom Provider neu vergeben. Das ständige Wechselspiel senkt die Gefahr einer Hacker-Attacke. Der Befehl *ipconfig* in der Eingabeaufforderung (*cmd*-Befehl unter *Ausführen*) ermittelt die lokale Rechneradresse ebenfalls. Die nächste Aufgabe besteht darin, die aktuellen Verbindungen samt Port-Belegungen zu überprüfen. Dafür gibt der User in der gleichen DOS-Box das Kommando *netstat -a* ein. Diese listet die Verbindung des eigenen Rechners mit fremden IP-Adressen auf sowie offene Ports. Mit dem Parameter *-n* stellt der User nur die aktiven Verbindungen dar. Um aus den kryptischen Kommunikationsdaten aber mögliche Angriffe präzise her-

auszufiltern, dient der Parameter *-o*. Windows zeigt dann auch die Prozess-ID des jeweiligen Tasks neben der IP-Adresse. Damit kann der Anwender Dienste beziehungsweise laufende Programme den belegten Ports zuordnen. Dafür öffnet der Nutzer den Taskmanager, ohne die DOS-Box zu schließen. Gleicht der Benutzer nun die PIDs im netstat-Fenster mit denen laufender Prozesse ab, springen mögliche Angriffe sofort ins Auge. Falls der Taskmanager die PIDs nicht standardmäßig listet, blendet der Anwender die Ordnungszahlen über *Ansicht/Spalten auswählen/PID (Prozess-IDs)* ein.

Die Umwandlung der jeweiligen IP-Adresse in den Namen des Hosts oder Webservers übernimmt das Kommando *tracert* in der DOS-Box. Die chronologische Ablaufverfolgung gibt darüber hinaus vage Hinweise auf die Entfernung des kommunizierenden Hosts.

Trifft der User tatsächlich auf fragwürdige Prozesse, gilt es, diese umgehend zu schließen. Das gelingt am einfachsten über den Taskmanager. Ist der Prozess beendet, schließt Windows auch den zugehörigen Port. Eine manuelle Korrektur ist nicht nötig.

## Druckerfreigabe und Netbios

Grundsätzlich sollte der Anwender die Dokument- und Druckerfreigabe deaktivieren und die Kommunikation per Netbios einschränken, falls er nicht in einem Netzwerk arbeitet. Netbios öffnet die Ports 135 bis 139, über die auch Trojaner Zugang erlangen können. Zunächst öffnet der Benutzer den Eigenschaften-Dialog der DFÜ- und Netzwerk-Verbindungen, markiert den Eintrag *Datei- und Druckerfreigabe für Microsoft-Netzwerke* und klickt auf *Deinstallieren*. Bei Bedarf richtet der User diesen Service später über *Installieren/Dienst* problemlos wieder ein.

Um Netbios zu deaktivieren, markiert der Benutzer in der gleichen Drop-down-Liste die Option *Internetprotokoll TCP/IP*. Anschließend klickt er auf den Button *Eigenschaften*. Im folgenden Fenster *Allgemein* wechselt der Anwender über *Erweitert* zu den Erweiterten TCP/IP-Einstellungen und klickt auf die Registerkarte *WINS*. Dort ist die Voreinstellung für Netbios auf *NetBIOS über TCP/IP deaktivieren* zu ändern und der Dialog zu schließen.

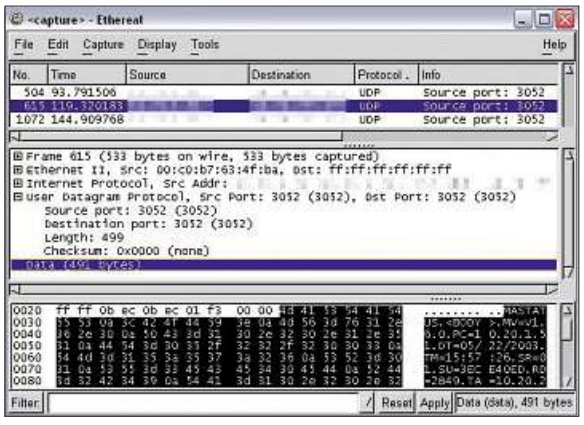
Die Gefahr, die durch offene Ports entsteht, sollte nicht unterschätzt werden. Denn ein Angreifer benötigt nur wenig Aufwand, um Zugang zu fremden PCs im Web zu erlangen. Hat der Hacker beispielsweise über einen Portscan ein mögliches Ziel gefunden, versucht dieser die Ordner-Freigabe des Opfers in die eigene Verzeichnisstruktur zu übernehmen (»mappen«). Das gelingt im Windows-Explorer über die Befehle *Extras/Netzlaufwerk verbinden* oder auf Kommandozeilen-Ebene mit *net use [Laufwerkbuchstabe]\\[IP-Adresse]\[Freigabename]*. Die erforderlichen Daten zum Opfer-PC erfährt der Hacker über professionelle Netzwerk-Utilitys und vorhandene Windows-Befehle wie *nbtstat*.

## Datenpakete überwachen

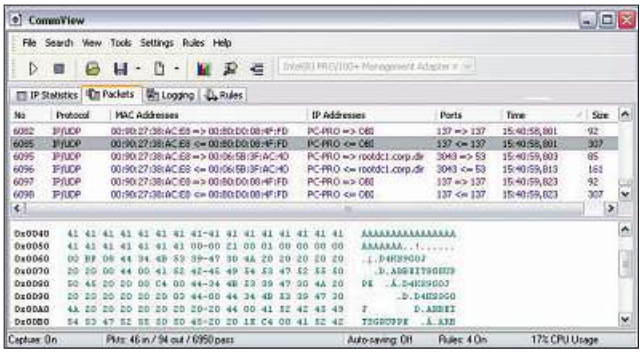
Hat der Anwender mögliche Angreifer ausgemacht, gilt es selbstverständlich, die Verbindung unverzüglich zu kappen. Besteht jedoch Unklarheit darüber, wer am anderen Ende der Leitung Kontakt aufnimmt und welche Daten der Rechner anfordert, sollten die Pakete genauer inspiziert werden. Spezielle Monitoring-Tools, auch als Sniffer bezeichnet, übernehmen diese Aufgabe. Allerdings erfordern die vom Sniffer gelieferten Protokolle ein grundlegendes Verständnis von TCP/IP.

Hinweis: Das Sniffen innerhalb geschlossener Netzwerk-Umgebungen ist aus Datenschutzgründen in der Regel verboten. Grundsätzlich sollte der Anwender deshalb zuvor den Administrator informieren.

Empfehlenswert ist hier die Freeware Ethereal *(www.ethereal.com)*. Diese zeichnet den kompletten Daten-Traffic auf und gewährt detaillierte Einblicke in die Pakete. Da das Programm im Capture-Modus mindestens 40 MByte Speicher raubt, sollte der Anwender auf eine Echtzeit-Darstellung der Pakete verzichten. Wer das Programm regelmäßig einsetzt, sollte zudem Filter definieren, nach denen beispielsweise nur bestimmte Pakete oder IP-Adressen erfasst werden. Für einen ersten Überblick ist es aber durchaus sinnvoll, Ethe-




◀ **Ethereal filtert auf Wunsch nur UDP-Pakete und stellt die Inhalte im unteren Fenster dar.**




**◀ Commview registriert die Netbios-Abfrage eines möglichen Angreifers über nbtstat sowie die bereitwillige Antwort des Opfers (unteres Fenster).**

real über die Befehle *Capture/Start* komplett alle Pakete mitschneiden zu lassen. Die Aufzeichnung sollte allerdings nicht mehr als zwanzig Minuten dauern, weil das Tool je nach Umfang der Daten ebenfalls mehrere Minuten braucht, um alle Pakete in die Listenübersicht zu laden. Letzteres geschieht automatisch, wenn der User den Capture-Prozess beendet. Im oberen Fenster stellt Ethereal die Verbindungen zwischen dem eigenen Host (Source) und dem Partner-Server (Destination) dar. Das verwendete Netz- oder Internet-Protokoll (Protocol) lässt Rückschlüsse auf die Art der verschickten Daten zu.

Einfacher lässt sich Commview *(www.commview.com)* bedienen – vor allem, was die Definition von Filtern anbelangt. Außerdem gibt sich Commview nicht so speicherhungrig, so dass eine Aktualisierung in Echtzeit möglich ist. In der kostenlosen Variante zeichnet der Netzwerk-Monitor zwar den kompletten Datenverkehr auf, lässt aber detaillierte Einblicke nur in jedes zweite Datenpaket zu.

## Verdächtig: ICMP, TCP, UDP

Von Interesse sind vor allem ICMP-Pakete (Internet Control Message Protocol), TCP-Pakete (Transmission Control Protocol) und UDP-Daten (User Datagram Protocol). Jeder Anwender kann über den ping-Befehl (ICMP) einen Server oder Host ansprechen, sofern die Zieladresse bekannt ist. Dabei werden kleine Datenpakete mit normalerweise 32 Bit Datenlänge verschickt, um zu überprüfen, ob der Zielrechner antwortet. Erhöht der Angreifer mit Hilfe eines so genannten Packet-Generators das Volumen auf über 64 KByte, kann dies zu einem Buffer-Overflow führen.

TCP-Pakete gelten als sicher, da diese über Prüfsummen authentifiziert und über Sequenznummern eindeutig zugewiesen werden. SMTP (Mails) und HTTP (Webseiten-Aufrufe) nutzen TCP-Kommunikation. Allerdings können auch Trojaner über TCP Kontakt aufnehmen. Insofern lohnt sich stets ein Blick in den Datenteil des Pakets. Das gilt in besonderem Maße auch für UDP-Messages.

Bei UDP fehlen Daten-Authentifizierung und Flusskontrolle. Damit können per UDP grundsätzlich ebenso unsichere und manipulierte Daten übertragen werden. Aus diesem Grund nutzen Hacker häufig UDP, um beispielsweise über eine falsche IP (IP-Hijacking) fremde Rechner abzuschießen oder Daten zu klauen. Auch hier sollte der Anwender im Verdachtsfall die Daten genauer inspizieren. Vor allem extrem große Datenpakete verdienen erhöhte Aufmerksamkeit. Einen Großteil der Gefahren wehrt die Firewall von Windows XP ab. Anhand der Pakettypen beziehungsweise der angeforderten Dienste entscheidet das Tool, ob die Pakete passieren dürfen oder nicht.

## XP-Firewall konfigurieren

Der User aktiviert die Firewall über die Eigenschaften der Netzwerk-Verbindung. Im Register *Erweitert* findet sich der entsprechende Eintrag. Mit einem Klick auf *Einstellungen* gelangt der Anwender zu den Optionen. Unter *Dienste* sollten alle Einträge deaktiviert sein, falls es sich nicht um einen Remote-PC handelt. Im Register *Sicherheitsprotokollierung* bestimmt der Benutzer, dass Windows die verworfenen Pakete aufzeichnet. Unbedingt leer bleiben sollten alle Kästchen im Karteireiter *ICMP*, da sich der User sonst gefährlichen Ping-Attacken aussetzen könnte. Mit einem Klick auf *OK* wird die Konfiguration beendet. Da es sich aber nicht um eine bidirektionale Firewall handelt, werden ausgehende Pakete nicht überprüft.

Anwender mit größeren Sicherheitsbedenken sollten daher zur bewährten Firewall Zone Alarm Pro *(www.zonelabs.com)* greifen, die auch in einer kostenlosen Version für den privaten Einsatz erhältlich ist und sich auf der Heft-CD befindet. OIB

# Überblick – Die Besten Tools für mehr Sicherheit

| Produkt | Eigenschaften | Internet | Preis |
|---|---|---|---|
| **Komplettpake gegen Adware, Spyware, Viren und Trojaner** | | | |
| Bösherz | Integriert Pop-up-, Inhalts-, Dialer- und Cookie-Blocker | www.boesherz-online.de | 7,50 Euro |
| Exe Blocker 1.5 | Regelwerk, nur vom User erlaubte Programme können starten | www.gamersunderground.de | kostenlos |
| Firewall Tester 3.0 | Testet Trojan-Blocker und zeigt, wie gut Sicherheits-Tools gegen Trojaner schützen | www.atelierweb.com | 25 Euro |
| Flow Protector | Reiche Ausstattung, Malware-Blocker, Content-Filter, Cookie- und Cache-Manager | www.flowprotector.com/de | 15 Euro |
| Ghostsurf Pro | Viele Zusatz-Features, Spyware-Blocker unter anderem mit Anonymizer-Funktion | www.tenebril.com | 40 Euro |
| Invisus PC Security | Erkennt 60 000 Malware-Tools von Trojanern über Adware bis zu Spyware | www.privacy4pc.com | 350 Euro |
| Pest Patrol 4.2 | Bewährt, bekämpft Ad-, Spyware, Keylogger, viele Trojaner und Denial-of-Service-Attacks | www.pestpatrol.com | 40 Euro |
| Popup Block | Spyware, Skripts und Pop-ups bekämpft dieses Tool | www.popupblock.net | 15 Euro |
| Proport Extreme | Kostenlos, Schutz gegen Trojaner, Backdoors, Spyware und Hack-Tools | www.tdupage.com | kostenlos |
| Safersurf | Anonym-Proxy schützt online gegen Web-Werbung, Spam, Dialer und Viren | www.nutzwerk.de | 5,90 Euro/Monat |
| Spy Remover 1.3 | Malware-Entferner gegen Spyware, Web-Bugs, Würmer, Cookies, Werbung und Skripts | www.itcompany.com | 20 Euro |
| Spyware-Adware-Remover | Echtzeit-Blocker gegen Spyware und Pop-ups, mit Adware-Remover | www.bulletproofsoft.com | 30 Euro |
| Virusscan Integrator | Mehr Virenschutz, die Software erlaubt, mehrere Viren-Tools gleichzeitig zu nutzen | www.handybits.com | kostenlos |
| Whats Happening 1.02 | Monitor, der versteckte Anwendungen übersichtlich anzeigt | www.turboware.com | kostenlos |
| X-Cleaner 2.0 | Anti-Spion, Spyware-Entfernung, User-Datenshredder und Spyware-Passcode-Breaker | www.xblock.com | 35 Euro |
| **Trojan-Blocker** | | | |
| $a^2$ Personal | Erkennt 10 000 Trojaner, gutes Tool mit Port-, Registry-, Disk- und Archiv-Scan | www.anti-trojan.net/de | 30 Euro |
| Anti-Hacker Expert 2003 | 12 000 Signature, scannt Ports, RAM, Registry und Festplatte | www.net2soft.com | 30 Euro |
| BO Clean 4.10 | Gegen 13 200 Trojaner, eliminiert Trojans komplett und schützt vor Trojan-Scans | www.nsclean.com | 35 Euro |
| Digital Patrol | 27 000 Viren und Trojaner registriert, mit Heuristik-Analyse, häufige Updates | www.antiviraldp.com | 25 Euro |
| System Safety Monitor | Verhindert auch DLL-Injections, sichert Windows gegen Systemänderungen | maxcomputing.narod.ru | kostenlos |
| Tauscan | Verständlich, leicht bedienbarer Schutz gegen die 1000 wichtigsten Trojaner | www.agnitum.com | 30 Euro |
| TDS-3 | 25 200 Trojaner registriert, bewährtes Spezial-Tool gegen Trojaner | tds.diamondcs.com.au | 50 Euro |
| The Cleaner Pro 4.0 | Drei-Wege-Schutz beim Download, in der Registry und per System-Scan | www.moosoft.com | 30 Euro |
| Zolt ZSM | Kontrolliert Windows Scripting Host, entfernt unerwünschte EXE-Files, auch für NT-Server | www.zolt.org | kostenlos |
| **Blocker gegen Adware, Spyware und Spionage-Software** | | | |
| Ad-Aware 6.1 | Hohe Erkennungsrate, aktuelle Version auch auf Deutsch erhältlich | www.ad-aware.net | kostenlos |
| Adware Agent 3.0 | Die 90 wichtigsten Spyware-Gruppen werden entfernt | www.killersoftware.com | 17 Euro |
| Goodbye Spy 4 | Vielseitiger Registry-Scan gegen Spyware und Spionage-Tools | www.tekeffect.com | 20 Euro |
| Internet Cleanup | Doppelpack, gegen Spyware und Spionage-Software einsetzbar | www.aladdinsys.com | 30 Euro |
| Snoopfree | Gegen Spione daheim und im LAN, Spezialisiert auf Spionage-Software | www.snoopfree.com | 20 Euro |
| Spy Sweeper 1.7 | Erkennt 1600 Spyware-Tools und wird laufend aktualisiert | www.webroot.com | 30 Euro/Jahr |
| Spyblocker 6.3 | Erprobter Blocker, erkennt rund 10 000 Spyware-Verbindungen und blockt diese | www.spyblocker-software.com | kostenlos |
| Spybot Search & Destroy | An User angepasst, besitzt Beginner- und Advanced-Mode, ständige Updates | security.kolla.de | kostenlos |
| Spyware Blaster 2.5 | Vorbeugung, verhindert die Installation von Spyware | www.wilderssecurity.net | kostenlos |
| Spyware Eliminator | Schutz vor Keyloggern, blockt bestimmte Spy- und Adware, keine Trial | www.aluriasoftware.com | 30 Euro |
| Spyware Guard 2.1 | Real-Time-Schutz mit Reporting | www.wilderssecurity.net | kostenlos |
| **0190- und 0900-Dialer-Blocker** | | | |
| 0190 Anti-Dialer | DFÜ-Monitor, überwacht Windows-DFÜ-Verbindungen | www.s-a-d.de | 10 Euro |
| 0190/0900-Warner | Zwei Versionen, überwacht alle aufzubauenden Verbindungen | www.wt-rate.com | kostenlos |
| 0190/0900 Alarm 3.70 | Zwei Versionen, überwacht alle aufzubauenden Verbindungen | www.aborange.de | kostenlos |
| Connectionwatch 2.5 | Umfangreich, Schutz-Tool inklusive der rechtlich wichtigen Protokoll-Funktion | www.connectionwatch.de | 23 Euro |
| Dial Guard 2.20 | Gegen internationale Dialer, englischsprachig, schützt vor Auslands-Dialern | www.dialguard.com/eng | 20 Euro |
| Dialer Scanner | Scannt und sendet verdächtige Malware ins Hersteller-Labor, mit Signatur-Update | www.dialerscanner.de | kostenlos |
| Dialer-Control 1.2.6 | Schutz vor Deaktivierung durch Dialer, überwacht alle Windows-Connects | www.dialer-control.de | kostenlos |
| Secuties PC Control | Komplette Protokollierung, Playback auf Wunsch, ferner Stealth-Mode | www.secuties.de | 15 Euro |
| YAW | Top-Scanner, mit Scan-, Quarantäne- und Smart-Update-Funktion | www.yaw.at | kostenlos |
| **Werbeblocker gegen Pop-ups, Banner und mehr** | | | |
| Ad Blocker 1.2 | Flash-Ads, Banner, Pop-ups und Cookies bekämpft dieses Tool | www.cdkm.com | 26 Euro |
| Ad Popup Killer 2.1 | Enhält mehr Features, inklusive IE-Cache-Cleaner und Log-Funktion | www.brothersoft.com | 16 Euro |
| Ad Substract Pro | Mit Werbungsstatistik, gut ausgestatteter Werbe- und Cookie-Blocker | www.adsubtract.com | 30 Euro |
| Anti-Popup Plus | Deutschsprachiger Pop-up-Blocker mit Datenshredder | www.kochmedia.de | 10 Euro |
| Filtergate | Rundumschutz gegen Banner, Tower-Ads, Pop-ups, Referer, Cookies und Web-Bugs | www.filtergate.com | 35 Euro |
| Freedom Pop-up-Blocker | Leistungsstark, blockt Online-Werbung fast komplett, mit Passwort- und Cookie-Manager | www.freedom.net | 30 Euro/Jahr |
| IE Popup Killer 2.0 | Für Internet Explorer, entfernt auch Flash-Pop-ups | www.fadsoft.com | 13 Euro |
| IP Ad Patrol 2.4 | Nachrichtendienst-Tool, verhindert Windows-Werbe-Pop-ups | www.tekeffect.com | 15 Euro |
| Just Stop Popups 5.0 | Günstig, erkennt unter anderem HTML-, PHP-, Javascript-, Perl- und XML-Werbung | deadbytetechnologies.com | 6 Euro |
| Pop Stopper | Nimmt Flash-Werbung ins Visier, gegen Pop-ups und Flash-Fenster | www.aluriasoftware.com | 20 Euro |
| Pop This 3.0 | Auch für Windows Instant Messenger, Instant Messaging werbefrei | www.mathies.com/popthis | kostenlos |
| Pop Up Blocker | Mit Clean-up, entfernt auf Wunsch Werbemüll auch aus dem Cache | www.guardprivacy.com | 7 Euro |
| Pop Up Cop 2.0 | Profi-Features: Meta-Refresh, Quellcode- und Cookie-Einstellungen | www.popupcop.com | 20 Euro |
| Popup Annihilator | Pop-up-Schutz mit Black- und Whitelist | solidlabs.com | 10 Euro |
| Pop-Up Stopper Pro | Blockt auch AOL-Pop-ups, Support für fast alle Browser | www.panicware.com | 30 Euro |
| Popup Vanish | Leicht bedienbar, User kann Whitelist erstellen | www.kalavath.co.uk | kostenlos |
| Popupagent 1.1 | Erkennt 5700 Spam-Sites, veränderbare Black- und Whitelist | www.spytech-web.com | 30 Euro |
| Stopzilla 3.0 | Konfigurierbar: Mit jedem geblockten Pop-up wird die editierbare Blacklist größer | www.stopzilla.com | 30 Euro |
| Webwasher Classic 3.3 | Ausgereift, gegen Werbung, Cookies, Web-Bugs, Referer, mit Inhaltsblocker | www.webwasher.com | kostenlos |
| Zap Ads | Kostenlos Werbebanner eliminieren | deadbytetechnologies.com | kostenlos |

# Online-Checks

**Mit Web-Audits lassen sich bis zu 1800 Hacker-Angriffe simulieren und Systeme auf individuelle Sicherheitslücken und Schwachstellen prüfen.**

Konstantin Breyer

Millionen verschiedener Konfigurationen von PCs im Web machen es Hackern leicht: Über seine individuellen Sicherheitslücken weiß kaum ein Anwender Bescheid, daher bleiben viele Rechner angreifbar. Das sollen Sicherheits-Audits im Internet verhindern. Diese simulieren Hacker-Angriffe und scannen offene Ports sowie aktive Trojaner. Anwendern liefern sie anschließend Anleitungen, wie alle gefundenen Sicherheitslücken zu schließen sind. Am besten erledigt der Testsieger Security Space diese Aufgaben. Neben anderen Tests simuliert dieses Audit besonders aktuelle Hacker-Angriffe *(www.securityspace.com/smysecure/last30.html)* und lässt sich am besten konfigurieren.

Einen Rundumschutz bietet aber keiner der getesteten Dienste. Vielmehr hat jeder seine eigenen Stärken. Spyware etwa findet *www.pestscan.de*. Viren und noch nicht aktive Trojaner werden insbesondere von Symantecs Security Check entdeckt. Aktive Trojaner erkennen im Test alle Dienste durch Portscans. Deswegen sollten Anwender mehrere Dienste gemäß ihren Bedürfnissen auswählen.




**▲ Auf der Webseite des empfehlenswerten Anbieters E-Soft unter www.securityspace.com sind 1800 kostenpflichtige Test verfügbar, die PCs und Netzwerk-Server auf Sicherheitslücken untersuchen.**

## Individuelle Gefahren

Sinnvoll ist der Einsatz der Web-Audits, weil jedes PC-System und jedes Netzwerk unterschiedliche Sicherheitslücken aufweist – selbst wenn dort die gleichen Betriebssysteme laufen. Ein Einzel-PC unter Windows XP, der bis zu einer Stunde täglich per ISDN online geht und Outlook sowie Internet Explorer nutzt, ist zum Beispiel in erster Linie von Viren, Spyware und Dialern bedroht. Ein LAN, das via DSL stets online ist und mehrere Betriebssysteme nutzt, wobei Internet- und Mail-Zugang via Router geregelt werden, zeigt andere Schwachstellen: Die größten Gefahren gehen hier von Hacker-Angriffen und Trojanern aus, die im zuvor genannten Beispiel nur eine untergeordnete Rolle spielen.

Vor allem FTP-, Filesharing- und Instant-Messaging-Tools bergen zusätzliche Sicherheitslücken, je nach Version und eingestellten Optionen. Interessante Beispiele auf *www.securityfocus.com*: FTP-Server-Besitzer können Systeme von Usern hijacken, die mit Cute FTP 5.0 Files downloaden. Die in Kazaa eingeblendete Werbung erlaubt ferner, unkontrolliert Skripte auf User-PCs auszuführen. Daher sollten Nutzer mindestens ein Security-Audit, besser mehrere, im Internet konsultieren. Unterlässt ein User dies, dann läuft er Gefahr, unerkannte Sicherheitslücken offen zu lassen oder eine überdimensionierte, zu teure Sicherheitslösung zu wählen, die ihn vor nicht relevanten Bedrohungen schützt. Einige Beispiele: Einen lokalen Virenscanner braucht jeder PC, doch eine Firewall bringt kaum etwas, wenn der User nur einmal am Tag kurz online geht, um Mails abzuholen. Wer per ISDN im Web surft, tut gut daran, einen Dialer-Blocker zu installieren. Wer ausschließlich DSL nutzt, braucht Letzteren hingegen nicht.

## Absturz möglich

Audits können, je nach Verbindung, zwei Stunden und mehr in Anspruch nehmen. Die meisten Audits bieten ausführliche Beschreibungen gefundener Sicherheitslücken sowie sinnvolle Anleitungen zu deren Beseitigung. User sollten nach Möglichkeit alle verfügbaren Tests ablaufen lassen, aber nie gleichzeitig am PC oder im LAN arbeiten. Je komplexere Hacker-Angriffe die Audits nachbilden, desto höher ist die Gefahr, dass die Online-Verbindung, das System oder das lokale Netz zusammenbrechen. Dies gilt vor allem für Denial-of-Service-Simulationen (DoS). Im *PC-Professionell*-Labor zeigen Logfiles von Always-online-Test-PCs, dass diese regelmäßig aufwändigen Hacker-Angriffen, darunter DoS, ausgesetzt sind. Durch DoS-Audits erfährt der User, an welchen Punkten sein System bei Angriffen instabil wird, und kann rechtzeitig sinnvolle Maßnahmen ergreifen. Gegen DoS-Attacken helfen nur Hardware-Firewalls. Ist der Angriff massiv genug, stürzen diese Firewalls zwar in der Regel ab, doch dadurch wird die Verbindung zum Internet und damit zum Angreifer gekappt. Der Schaden begrenzt sich also im schlimmsten Fall auf eine Offline-Periode bis zum manuellen Reboot der Firewall. Bei einer Desktop-Firewall ist ein Absturz des PCs möglich.

## E-Soft Security Space

Neben der kostenpflichtigen Buchung von Accounts ab 10 Euro *(www.securityspace.com)* ist der Start aller Tests per Einzelauswahl kostenlos möglich. Features wie zeitgesteuerte Scans und ein Jahr lang abrufbare Protokolle machen den Wert der kostenpflichtigen Accounts aus. Ständig werden rund 1800 simulierte Angriffe durch aktuelle ergänzt. Konfiguration und Support sind sehr gut, die Erklärungen zu Sicherheitslücken treffend und verständlich. Nutzer sehen stets den aktuellen Stand des Audits. Einziges Manko: Bevor das 102-Minuten-Audit startet, muss der User je nach Auslastung bis zu zwei Stunden warten. Insgesamt ist das Audit für Privat- und Firmennutzer sehr empfehlenswert.

## Symantec Security Check

Übersichtlich und verständlich zeigen sich Oberflächen und Texte dieses Audits unter der Adresse *security.symantec.com/de*. Obwohl nur 134 Portscans ablaufen, sind fast alle für Einzel-PCs besonders relevanten Gefahren erfasst. Eine Konfiguration ist nur begrenzt möglich, doch ist dies kaum von Nachteil, da




▲ **Nutzerfreundlich und verständlich: die Oberfläche von Symantec Security Check.**

der Zeitaufwand für den User beim kompletten Durchlauf ohnehin niedrig ist. Die ansonsten durchschnittliche Ausstattung wird durch Scans auf aktive und inaktive Trojaner sowie Viren gut ergänzt. Da nur Symantec diese Kombination von Online-Audits gegen Hacker und Viren bietet, ist es für User sinnvoll, Symantec Security Check zumindest zusätzlich zu anderen Audits zu nutzen. KBR

## Malicious-Code-Scans: Viren & Dialer finden

Viren und Spyware werden von vielen Anti-Hacker-Audits ignoriert. User sollten hierfür zusätzliche Web-Dienste nutzen, dabei aber schwarzen Schafen ausweichen. Per Mail, durch Usenet- und Filesharing-Downloads sowie beim Surfen gelangen oft unbemerkt schädliche Skripte und Programme auf den PC: Viren, Trojaner, Spyware und Dialer. Nur der Anti-Hacker-Check Audit-my-PC erkennt auch Spyware. Mehr Audits gegen Spyware gibt es nicht, weitere Infos liefern nur Tools wie Adaware *(www.lavasoft.de)*. Allein Symantec Security Check findet beim Audit auch Viren sowie Trojaner, die noch inaktiv in den Download-Ordnern schlummern. Doch Viren und inaktive Trojaner spüren auch weitere Spezial-Audits auf. Dabei haben User die Wahl zwischen sieben kostenlosen Angeboten. Kostenpflichtigen Online-Scans ist ein lokaler Scanner vorzuziehen: Lokale Tools schützen umfassender und zuverlässiger, etwa wenn gerade keine Online-Verbindung besteht. Kostenlose und gleichzeitig seriöse Online-Scans bieten neben Symantec unter anderem folgende Firmen:

- Bitdefender *(www.bitdefender.com)*
- Command *(www.commandondemand.com)*
- Freedom *(www.freedom.net)*
- Panda (www.pandasoftware.com),
- RAV *(www.ravantivirus.com)*
- Trend Micro *(housecall.trendmicro.com)*

Bei jedem dieser Dienste ist der Download von Plug-ins nötig. User sollten darauf achten, nur von diesen Anbietern solche Plug-ins zu akzeptieren. Unter einigen anderen Webadressen, beispielsweise unter *www.secure-me.net*, versuchen unseriöse Anbieter, Usern statt Scan-Plug-ins gefährliche 0190-Dialer unterzuschieben.

Kaum Testmöglichkeiten finden User gegen Dialer, die bereits im eigenen System sein können. Der einzige Dialer-Check im Web *(www.nutzwerk.de/saferurf)* analysiert nur, wie leicht ein Dialer auf die lokale Festplatte gelangt. Gegen Dialer sollten Anwender daher auf eine spezialisierte Software, beispielsweise auf YAW 3.5 *(www.yaw.at)* oder 0190/ 0900-Warner 4.0 *(www.wtrate.de)* zurückgreifen.

# XP-Sicherheit

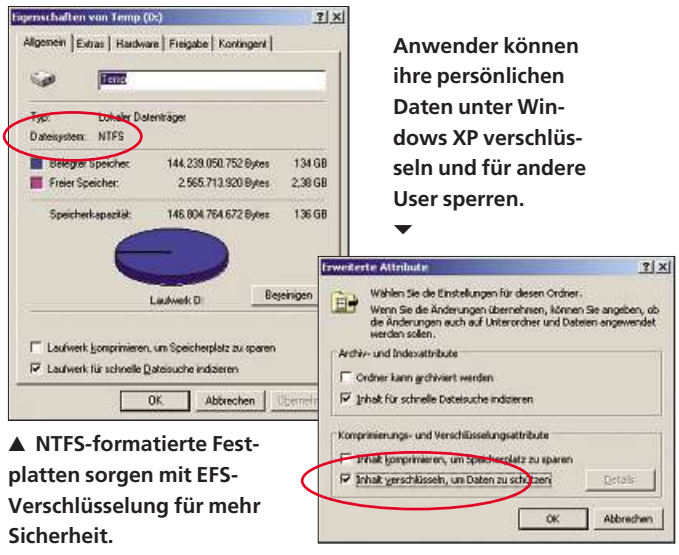
**Windows 2000 und XP lassen sich mit wenigen Handgriffen gegen die meisten Gefahren aus dem Web schützen. PC Professionell nennt die wichtigsten Tipps.**

Oliver Ibelshäuser

Firewall und Virenscanner sind im täglichen Einsatz unverzichtbar, blocken aber letztlich nur bekannte Viren oder Hacker-Angriffe, die nach einem bestimmten Muster ablaufen. So finden zahlreiche Malware-Programme noch immer offene Türen ins System. Das liegt unter anderem daran, dass diese rechtlich nicht immer eindeutig den Schadensprogrammen zuzuordnen sind wie beispielsweise Dialer oder vom Virenscanner überhaupt nicht als Malware wahrgenommen werden. Das gilt für Webbugs, ActiveX-Controls und Cookies. Die Aufgabe, sich dieser Plagen zu entledigen, bleibt beim Anwender.

## NTFS: Sicherheit und Privatsphäre

Wer Windows XP oder Windows 2000 auf einem Einzel-PC im Einsatz hat, sollte für die Systempartition das sichere Dateisystem NTFS wählen. Die Verwaltung großer Datenmengen ist komfortabler, die Wiederherstellung zerstörter Daten deutlich ergiebiger. Und bei den aktuellen Taktraten der PCs ist auch kein Geschwindigkeitsverlust gegenüber FAT32 spürbar. Für die Konvertierung empfiehlt sich etwa Partition Magic 8, das nun von Symantec verkauft und weiterentwickelt wird. Allerdings sollte der Anwender zuvor unbedingt ein Image anlegen, um Fehler beim Datentransport auszuschließen.




▲ **NTFS-formatierte Festplatten sorgen mit EFS-Verschlüsselung für mehr Sicherheit.**

**Anwender können ihre persönlichen Daten unter Windows XP verschlüsseln und für andere User sperren.**

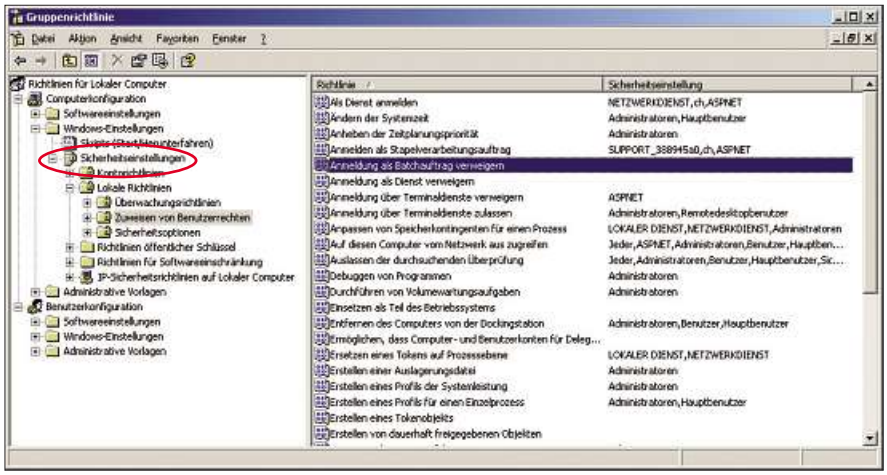
NTFS-Anwender kommen in den Genuss verschlüsselter Ordner und Dateien. Davon profitieren Sie nicht nur, wenn Sie ihren PC mit anderen Anwendern teilen oder einem Administrator Zugriff auf sämtliche Daten gewähren müssen. Die Verschlüsselung schützt auch vor dem Verlust sensibler Daten bei einer Infektion durch einen Trojaner.

Um Ordner zu verschlüsseln, reicht es aus, über die Eigenschaften auf den Button *Erweitert* zu klicken und im Dialog *Erweiterte Attribute* auf *Inhalt verschlüsseln* zu klicken. Die künftige Ver- und Entschlüsselung der Daten ist an den Benutzer-Account gebunden. Wer sich mit einem anderen Benutzernamen einloggt, sieht bei den geschützten Daten nur wirren Zeichensalat. Obwohl die (De)Codierung in Echtzeit geschieht, ist es ratsam, diesen Schutz auf persönliche Daten zu beschränken. Systemeinstellungen, Bookmarks oder ganze Anwendungen sollten nicht codiert werden. Beim Kopieren der Daten auf einen externen Datenträger oder beim Brennen geht die Codierung übrigens verloren.

Tipp: Um einen Überblick über die verschlüsselten Ordner zu erhalten, empfiehlt es sich, die Verzeichnisse farbig zu markieren. Das erledigt der Datei-Explorer über *Extras/Ordneroptionen/Ansicht* und einen neuen Haken vor der Option *Verschlüsselte oder komprimierte NTFS-Dateien in anderer Farbe anzeigen*.

## Surfen mit beschränkten Rechten

Allein für das Surfen im Web lohnt es sich, ein zweites Benutzerkonto mit eingeschränkten Rechten anzulegen. Windows verwaltetet diesen Typus als Benutzer, im Gegensatz zum




◀ **Mit Sicherheitseinstellungen können Administratoren die Sicherheitsrichtlinien für jeden Benutzer ändern und individuelle Zugriffsrechte festlegen.**

Administrator mit uneingeschränkten Rechten. Hintergrund: Der Benutzer darf zwar in vielen Fällen auch Programme installieren, diese gelten aber nur für das eigene Profil. Zudem dürfen Windows-Benutzer keine Änderungen an Systemdateien oder der Registry vornehmen, die auch andere Anwender betreffen. Diese Restriktionen haben einen positiven Nebeneffekt. Wer sich beim Surfen einen Virus, ein schadhaftes ActiveX-Control oder eine Spyware einfängt, stoppt den Wirkungskreis der Malware. Diese kann dann weder Systemdateien patchen noch einen Stempel in der Registry hinterlassen. Über die Gruppenrichtlinien *(gpedit.msc /a)* lassen sich die Beschränkungen unter *Windows-Einstellungen/Sicherheitseinstellungen/Lokale Richtlinien/Zuweisen von Benutzerrechten* noch verfeinern, indem der Benutzer aus den dort aufgeführten Berechtigungen entfernt wird.

## Kontrolle über Startdateien und Dienste

Nahezu jedes schadhafte Programm, das sich auf dem Rechner einnistet, hinterlegt einen Startaufruf in der Registrierdatenbank oder im Autostartordner. Es ist daher dringend geboten, die Liste der Dateiaufrufe regelmäßig einzusehen. Am einfachsten gelingt das über das Systemkonfigurations-Programm, das der Anwender über den Befehl *msconfig -6* aufruft. In diesem Fall gelangt der User ohne Umwege zum Katalog der Systemstarteinträge, die neben dem Autostart-Ordner auch die Run-Keys aus *Hkey_Local_Machine* und *Hkey_Local_User* umfassen. In der Leiste *Befehl* findet sich der Dateipfad, der in der Regel bereits Rückschlüsse auf den Urheber des Programms zulässt. Im Zweifelsfall sollte der Anwender die zugehörige Datei lokal im System ausfindig machen und über die Dateieigenschaften oder eine Internet-Recherche weitere Informationen einholen. Bestehen berechtigte Zweifel an der Integrität des Startaufrufs, sollte der Anwender das File nicht löschen, sondern auslagern oder die Extension auf *TXT* ändern, was die Datei unschädlich macht, aber nicht zerstört.

Einen Sicherheits- und Komfort-Check verdienen ebenfalls die Services, die Windows unter der benachbarten Registerkarte *Dienste* zusammenfasst. Aus Sicherheitsaspekten interessant sind zunächst Dienste, die nicht von Microsoft stammen. Über die Optionen *Alle Microsoft-Dienste ausblenden* verkleinert der Anwender die Auswahl. Wenn die Bezeichnung des Services nicht ausreicht und unter Hersteller die Meldung *Unbekannnt* auftaucht, bietet es sich an, diesen Dienst testweise zu deaktivieren.

Von den Microsoft-Diensten sind folgende entbehrlich, wenn der Anwender nicht in einer Netzwerk-Umgebung arbeitet: *Ablagemappe, Anmeldedienst, Computerbrowser, Hilfe und Support, Intelligenter Hintergrundübertragungsdienst, Nachrichtendienst, NetMeeting-Remotedesktopfreigabe, NLA, QoS-RSVP, Remote-Registrierung, Sekundäre Anmeldung, Seriennummern der tragbaren Mediengeräte, Server, Sitzungs-Manager für Remotedesktophilfe, Treibererweiterung für Windows Verwaltungsinstrumentation, Überwachung verteilter Verknüpfungen, Warndienst, Webclient, Windows-Zeitgeber*.

Tipp: Sinnvollerweise sollte die detaillierte Konfiguration der Dienste über das Snap-in Dienste *(services.msc)* geschehen, da hier die Abhängigkeiten eingesehen werden können.

## Überwachung laufender Prozesse

Der Taskmanager listet alle aktiven Prozesse auf – auch solche, die vom System als versteckt

markiert sind. Allerdings sind die Informationen recht spärlich. Um zu überprüfen, welche laufenden Tasks Verbindung zur Außenwelt aufnehmen, muss das Tool zunächst über *Ansicht/Spalten auswählen/PID* die Prozess-ID jedes Tasks einblenden. Dann startet der Anwender den Befehl *netstat -o* in der Shell *(cmd)*. Alle Netzwerk- und Internet-Verbindungen werden nun samt der zugehörigen PID und der IP-Adresse des verbundenen Servers oder Clients gelistet. Über den Abgleich der PIDs erfährt der Anwender ohne Umweg, ob sich aktive Spyware, Adware oder Würmer im System verstecken

Was die lokal laufenden Tasks bewirken, die aktuell keine Verbindung ins Internet haben, kann diese Methode allerdings nicht aufdecken. Hier hilft aber der Process Explorer von Sysinternals *(www.sysinternals.com)*. Das Tool nennt die von jedem Task und jeder aktiven Datei vorgenommenen Zugriffe auf die Registry sowie auf diverse andere Dateien, Ordner und Dienste, Ports, Windows-Komponenten und Threads.

## Internet Explorer abschotten

Die meisten Türen in das Windows-System öffnet der Internet Explorer 6. Dennoch gibt es keine einheitliche Empfehlung für eine Sicherheitskonfiguration des Web-Browsers. Der Grund: Allzu restriktive Einstellungen gehen zu Lasten des Komforts. Wer grundsätzlich kein Javascript akzeptiert und Cookies blockiert, wird zahlreiche Internet-Seiten gar nicht oder nicht vollständig darstellen können. Insofern hängen die optimalen Werte immer von den persönlichen Surf-Präferenzen ab.

Relevante Einstellungen finden sich im Register *Sicherheit*. Hier wählt der Anwender den Button *Stufe anpassen*. Sinnvoll sind Korrekturen bei den Scripting-Einstellungen. Den Eintrag *ActiveX-Steuerelemente ausführen, die für Scripting sicher sind*, deaktivieren vorsichtige Anwender. Im schlimmsten Fall reagiert eine entsprechende Webseite dann mit einer Fehlermeldung, wenn diese versucht, eine Komponente auf die Festplatte zu laden. Zudem sollte die Option *ActiveX-Steuerelemente und Plug-ins ausführen* von *Aktivieren* auf *Eingabeaufforderung* gesetzt werden, um größtmögliche Sicherheit beim Surfen zu erlangen. Darunter könnte allerdings der Komfort leiden, da viele Portale wie AOL den Anwender mit Abfragedialogen überhäufen.

Zudem sollte der Anwender aus Sicherheitsgründen folgende Optionen deaktivieren: *Download von signierten ActiveX-Controls, Download von nicht signierten ActiveX-Controls, Einfügeoperationen über Skript zulassen, Scripting von Java-Applets, Scripting von Java-Applets, Dauerhaftigkeit von Benutzerdaten, Installation von Desktopobjekten, Metafresh zulassen*.

Nicht minder wichtig ist die Aufgabe, regelmäßig den Internet-Müll zu löschen, die platzierten ActiveX-Controls zu überprüfen und gegebenenfalls zu eliminieren. Zunächst kümmert sich der User um die Reste der letzten Surf-Touren unter *Extras/Internetoptionen/Temporäre Internetdateien und Cookies löschen*. Nach den Dateien im gleichen Register sind die Objekte dran. Zuvor sollte sich der Benutzer überzeugen, dass keine erwünschten ActiveX-Controls unter diesen Objekten sind. Online-Virenscanner speichern üblicherweise ActiveX-Programme auf der Festplatte, ohne die eine Virensuche nicht funktioniert. Dazu genügt ein Klick auf *Einstellungen und Objekte zeigen*. Allein die URL der Ursprungsseite sollte für Klarheit sorgen. Mehr Informationen – etwa zum Hersteller des Programms – lassen sich über *Eigenschaften* (rechte Maustaste) abrufen. HME




In den Internetoptionen des Internet Explorers sollten Anwender Sicherheitszonen für das Web definieren.




Das Abschalten von aktiven Inhalten sorgt für mehr Sicherheit zu Lasten des Bedienkomforts.

# Windows-98-Schutz

**Microsoft hat den Support für Windows 98 und Me eingestellt. Anwender müssen nun selbst Vorsorge treffen und sich mit Tools für mehr Sicherheit schützen.** Stefan Greiner

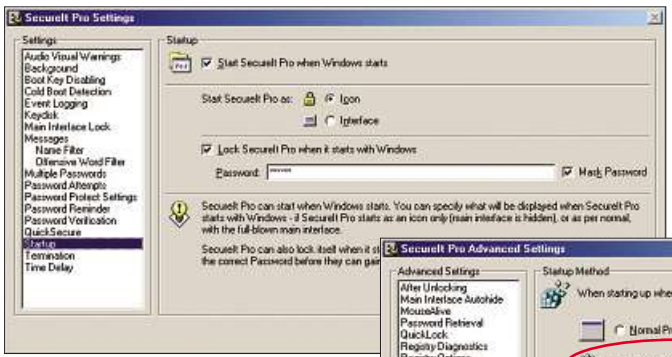
Das für das erste Halbjahr 2004 angekündigte Servicepack 2 für Windows XP wird neue Versionen von Internet Explorer und Outlook Express enthalten. Diese sollen Sicherheitslücken schließen und es Angreifern künftig erschweren, in fremde Systeme einzubrechen. Anwender von Windows 98 und Me werden von der Verbesserungen nicht mehr profitieren. Denn Microsoft hat den Support zum 16. Januar 2004 aufgekündigt und stellt via Online-Update keine Aktualisierungen mehr zur Verfügung. In der Praxis sind Anwender nun selbst gefordert, um Windows 98 und Me auch weiterhin ohne Sicherheitslecks nutzen zu können und die Gefahr von Hacker-Attacken zu minimieren.

Doch nicht nur Schwächen im integrierten Browser und Mail-Client sind bedenklich. Fehlende Verschlüsselung und Firewall, eine unzureichende Benutzerverwaltung und der mangelhafte Schutz von User-Daten öffnen Angreifern Tür und Tor. Microsoft bietet hier keine passenden Lösungen an, sodass Anwender zu Programmen aus der Free- und Shareware-Szene greifen sollten.

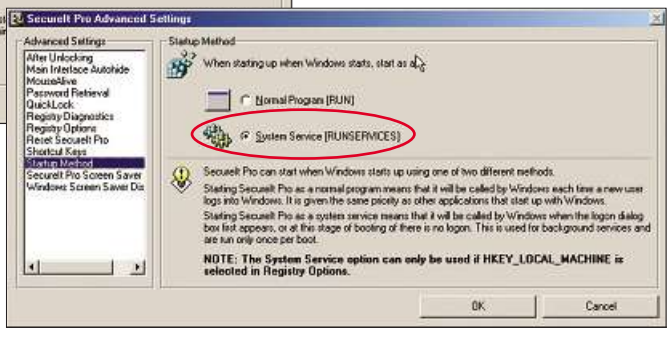
Windows 98 und Me sind DOS-basierte Betriebssysteme, die Angreifern – etwa feindlich gesinnten Kollegen – auch ohne Anmeldename und Passwort einen einfachen Zugang zu den Daten erlauben. Dazu muss lediglich beim Start ein neuer User angelegt und ein beliebiges Passwort vergeben werden. Da eine Verschlüsselung fehlt, sind alle Daten anderer Benutzer frei zugänglich. Der erste Schritt ist daher, den Zugang mit einem Bios-Passwort einzuschränken. Das bietet zwar auch keine hundertprozentige Sicherheit, erschwert den Zugang aber zumindest, da der Angreifer über fundiertes technisches Know-how verfügen muss.

## Zugang einschränken

Das Freeware-Programm Secure IT Pro 4.70 *(www.quantrix.net)* integriert zahlreiche Funktionen, um Windows zu schützen. So lässt sich das Tool beispielsweise als Windows-Service starten, der vor dem Anmeldedialog von Windows gestartet wird und ein zuvor vom Anwender festgelegtes Passwort verlangt. Ein




Secure IT bietet zahlreiche Optionen, mit denen der unbefugte Zugang zu einem Windows-98 und -Me-System wirksam unterbunden werden kann.




Wird Secure IT als Windows-Service gestartet, erscheint vor dem »normalen« Anmeldedialog von Windows eine zusätzliche Passwort-Abfrage.




**▲ Die Freeware Easy Crypto Deluxe 5.5 verwendet die sichere Blow-Fish-Methode zum Verschlüsseln von beliebigen Dateien und Verzeichnissen.**

Umgehen der Abfrage durch einen Windows-Start im abgesicherten Modus nach dem Beenden von Windows per [Strg Alt Del] oder Reset-Schalter kann blockiert werden.

Außerdem ist es möglich, einen sicheren Screensaver aufzurufen, der das System in Abwesenheit des Anwenders gegen einen unbefugten Zugang sichert. Das Programm ist sehr empfehlenswert und bietet genau die Sicherheitsoptionen, die Windows 98 und Me von Haus aus vermissen lassen.

Das ebenfalls kostenlose Tool Winguard Pro 2004 Free Edition *(www.winguardpro.com)* bietet dem Windows-User beispielsweise die Möglichkeit, Programme mit einem Passwort vor dem Aufruf zu schützen. Im *Advanced*-Register können Anwender den Desktop mit einem Passwort sperren. Alle Sperren bleiben nach einem Systemneustart aktiv.

## Datenverschlüsselung

Windows 98 und Me integrieren von Haus aus keine Datenverschlüsselung. Diese lässt sich aber sehr einfach nachrüsten. Ein empfehlenswertes Programm hierzu ist Easy Crypto Deluxe 5.5 *(www.handybits.com)*. Das für den privaten Einsatz kostenlose Programm arbeitet mit dem Blow-Fish-Algorithmus, der einen 128 Bit langen Schlüssel verwendet. Nach der Installation bindet sich das Tool als Windows-Shell-Erweiterung in das Explorer-Kontextmenü ein und stellt dort die Funktionen *Verschlüsseln* und *Zu Easy Crypto Zip* bereit. Im Programm selbst wählen Nutzer die Verschlüsselungsfunktion, vergeben ein neues Passwort oder beziehen eines aus der zuvor definierten Passwortliste und wählen die entsprechende Datei aus. Die Originaldateien werden so gelöscht, dass sie auch mit Spezial-Tools nicht mehr hergestellt werden können. Auch komplette Ordner mit allen darin befindlichen Dateien lassen sich mit einem Klick verschlüsseln. Zur Weitergabe der verschlüsselten Archive als selbstentpackende EXE-Datei dient die Option *Archiv erzeugen*. Der Empfänger benötigt nur das Passwort, um die Dateien zu entpacken und entschlüsseln.

## Alternativen für Internet Explorer und Outlook Express

Die größte Schwachstelle von Windows und erklärtes Angriffsziel für Hacker sind Internet Explorer und Outlook Express. Fast täglich werden neue Sicherheitslücken bekannt, die von Microsoft per Online-Update geschlossen werden. Das gilt zukünftig aber nur noch für Windows 2000 und XP – User von Windows 98 und Me werden nicht mehr mit aktuellen Patches versorgt. Außerdem fehlt dem Internet-Explorer ein Pop-up-Blocker, der erst in der nächsten Version enthalten sein soll. Der sicherste Weg ist daher ein Umstieg auf Gratis-Alternativen.

Der schlanke Browser Firebird (deutsche Version unter *www.firebird-browser.de*) zeigt keine Anfälligkeiten für aktive Webkomponenten wie beispielsweise ActiveX-Controls oder andere Script-Sprachen. Für zusätzliche Sicherheit sorgt der Pop-up-Blocker, der unaufgefordert geöffnete Browserfenster automatisch schließt. Auch Opera *(www.opera.com)* ist weniger anfällig für Attacken und integriert ebenfalls einen Pop-up-Blocker.

Mehr E-Mail-Sicherheit bietet der Open-Source-Mail-Client Thunderbird *(thunderbird.diepause.de)*, da die Entwickler auf eine eigene Engine zur Anzeige HTML-formatierter Nachrichten setzen. Daher laufen Wurmattacken ins Leere. Thunderbird integriert außerdem einen lernfähigen Spam-Filter. Ähnliche Funktionen wie Thunderbird bietet Pegasus Mail 4.12 *(www.pmail.com)*.

## Firewall und Virenschutz

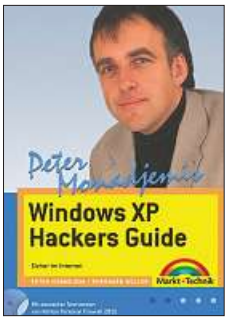
Für wirksamen Schutz gegen Hacker-Attacken und Viren sollten unbedingt entsprechende Programme installiert sein. Die Empfehlungen der *PC-Professionell*-Redaktion sind Sygate Personal Firewall Pro 5.5 (siehe Test auf Seite 63) und Panda Antivirus Platinum 7 (siehe Test auf Seite 50). Kostenlose Alternativen wie AVG Free Edition und Sygate Personal Firewall Standard finden sich auf der Heft-CD zu dieser Ausgabe. HME

## Buch-Tipps der Redaktion zum Thema »Sicherheit«



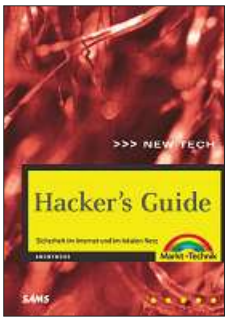

**Othmar Kyas/Markus a Campo**
**IT-Crackdown**
Wie funktioniert eine Risikoanalyse? Was ist beim Aufbau einer Unternehmens-Sicherheitsarchitektur zu beachten? »IT-Crackdown« beleuchtet die Architektur von Internet und Intranet und gibt dem Leser Tipps zum Schließen von Sicherheitslücken unter allen gängigen Betriebssystemen.

Mitp, ISBN 3-8266-0848-8, 560 Seiten, 35 Euro



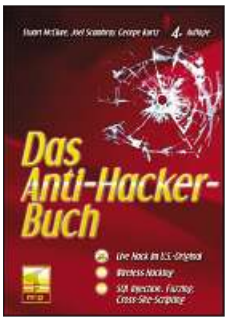

**Peter Monadjemi**
**Windows XP Hackers Guide**
Die Sicherheit von Windows XP steht im Mittelpunkt von Peter Monadjemis neuestem Werk: Schutz von Viren, Würmern und Trojanern, der Einsatz von Personal Firewalls, das Schließen von Sicherheitslücken sowie das Verwischen von Spuren im Internet erklärt der Autor Schritt für Schritt.

Markt &Technik, ISBN 3-8272-6538-X, 25 Euro




**Anonymous Hacker's Guide**
Der beste Schutz von PCs und Netzwerken ist das Wissen um die Denkweise der Angreifer: »Hacker's Guide« zeigt die Methoden und Tricks der Hacker und wie diese mit ihren eigenen Waffen zu schlagen sind. Die Neuauflage beleuchtet aktuelle Sicherheitstrategien, Absicherungskonzepte und Tools.

Markt &Technik, ISBN 3-8272-6522-3, 1032 Seiten, 40 Euro




**McClure/Scambray/Kurtz**
**Das Anti-Hacker-Buch**
»Das Anti-Hacker-Buch« versteht sich als Präventivschlag gegen das unerlaubte Eindringen in Netzwerke aller Art: Schwachstellen von WLAN-Netzwerken, Apache- und IIS-Systemen werden ebenso erklärt wie Strategien zum Schutz vor Dial-Up-, PBX-, Voicemail und VPN-Hacks.

Mitp, ISBN 3-8266-1375-9, 840 Seiten, 40 Euro



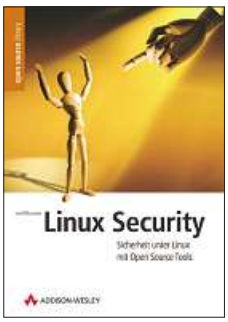

**Markus a Campo**
**Sicherheit total**
Ob Online-Banking, 0900-Dialer oder Spam: Das Buch vermittelt theoretisches wie praktisches Wissen, um Sicherheitslücken aller Art aufzuspüren und zu schließen - richtet sich dabei insbesondere an Anwender und Unternehmen, die sich keine finanziell aufwändige Sicherheitslösung leisten können.

BHV, ISBN 3-8266-8119-3, 750 Seiten, 20 Euro




**Spenle/Czichowski/Steinhoff**
**Windows Sicherheit**
Dieses Buch macht Anwender mit den Elementen des Windows-Sicherheitssystems vertraut und hilft somit, die richtigen Sicherheitsrichtlinien zu entwerfen und umzusetzen. Mit Praxistipps zu Kryptographie, Microsoft-Hotfixes und -Service-Packs sowie zur Erstellung eines Notfallplans.

Data Becker, ISBN 3-8158-2518-0, 690 Seiten, 50 Euro




**Josef Brunner**
**Linux Security**
»Linux Security« dient als Helfer, um Linux-Systeme gegen Hacker abzusichern: Der Autor erklärt, mit welchen Tricks Hacker in fremde Systeme eindringen und zeigt, wie dies mit kostenlosen Open-Source-Tools wie LIDS, Snort, N-Map, Webmin oder Nessus verhindert werden kann.

Addison-Wesely, ISBN 3-8273-1999-4, 522 Seiten, 50 Euro




**Howard/LeBlanc Writing**
**Secure Code**
Die Autoren – beide Sicherheits-Experten – zeigen mit »Writing Secure Code«, wie wichtig der Aspekt Sicherheit bereits bei Programm-Entwicklung und -Design ist. Code-Beispiele und Security-Checklisten helfen Programmierern, robuste und sichere Software zu entwickeln. (Englischsprachig)

Microsoft Press, ISBN 0-7356-1722-8, 770 Seiten, 47 Euro

# Abhörsicher

**VPN-Gateways auf IPsec-Basis verbinden Firmennetze schnell und sicher übers Internet. Und dies günstiger als mit einer Festnetz-Verbindung.**

Dr. Andreas Anton Bloom

Bei der Vernetzung zweier LANs sind Virtuelle Private Netzwerke (VPN) kostengünstige Alternativen zu Standleitungen. Mitarbeiter von Unternehmensstandorten oder Heimarbeiter können so über das Web auf Daten in der Firmenzentrale zugreifen. Damit die Sicherheit dabei nicht zu kurz kommt, werden die Daten via IPsec verschlüsselt übertragen. IPsec kann sich hierfür prinzipiell aller Verschlüsselungsalgorithmen bedienen. Allerdings ist DES beziehungsweise 3DES die Mindestvoraussetzung für den sicheren Datenverkehr.

Dazu bedarf es nicht nur wie bisher eines Routers, sondern auf beiden Seiten eines IPsec-Gateways (Internet Protocol Security) zur Ver- und Entschlüsselung der Daten. Das Gateway benötigt nach wie vor einen Router. Intelligentere Konzepte kombinieren Routing- sowie VPN-Funktionalitäten in einem Gateway. Für IPsec-basierte Verbindungen muss der Anwender mit einer höheren Investition rechnen als für ein einfaches Gateway. Die Preise beginnen bei rund 800 Euro.

Werden lediglich zwei einfache Netzwerke, in denen sämtliche User die gleichen Rechte haben, miteinander verbunden, reicht im Grunde ein preiswertes IPsec-Gateway, das nur mit Preshared Keys arbeitet (Sicherheitsschlüssel). Weichen die Anforderungen wie im Falle mehrerer Sub-Netze jedoch auch nur geringfügig von dem einfachsten Fall ab – und das ist gerade im professionellen Anwendungsumfeld fast immer der Fall –, dann kann der Administrator Schwierigkeiten bekommen. Vor allem, wenn er sich eines Low-Cost-Produkts bedient. Im Folgenden werden einige Problemstellungen beschrieben, die der Anwender für den Aufbau einer IPsec-basierten Datenverbindung in jedem Fall berücksichtigen sollte.




▲ **Sichere Verbindung: Aus dem Außenstellen-LAN wird nur der Traffic durch den IPsec-Tunnel 192.168.1.0 / 24 zugelassen.**

## Flexibilität durch IP-VPNs

Damit nicht gleich die gesamte Struktur der zu verbindenden LANs geändert werden muss, sollte sich ein IPsec-Gateway nahtlos in die vorhandene Infrastruktur einfügen - und nicht umgekehrt. So muss das Gateway die Möglichkeit bieten, die innerhalb einer einzigen Filiale vorliegenden verschiedenen Sub-Netze beziehungsweise alle verwendeten IP-Sub-Netz-Adressräume zu unterstützen. Dieses wird über mehrere gleichzeitige IPsec-Tunnel realisiert (»Multiple Policy Support«). Das verhindert, dass alle PCs in das gleiche Sub-Netz verschoben werden.

Zur Anbindung zweier Standorte über IPsec ist es notwendig, den Gateways die IP-Adressen des Partner-LANs mitzuteilen. Bei der Vernetzung von zwei PCs reicht es aus, wenn der Benutzer lediglich einen Adressraum pro Partnernetz angibt. Verfügt jedoch ein Standort über zwei voneinander getrennte Sub-Netzwerke (zum Beispiel für den Vertrieb und die Fertigungsabteilung), erweisen sich einfache VPN-Gateways um die 100 Euro in der Praxis als ungeeignet.

Ein professionelles IPsec-Gateway sollte in der Lage sein, mehrere Policies beziehungsweise Traffic-List-Einträge pro Peer (Partnernetz) zu unterstützen. Eine solche Policy

stellt eine Sammlung verschiedener Selektoren wie IP-Adresse, IP-Sub-Netz, Protokoll oder Port dar. Damit lässt sich exakt definieren, welcher Traffic, wie beispielsweise Datenverkehr aus einem oder mehreren Sub-Netzen, verschlüsselt werden soll.

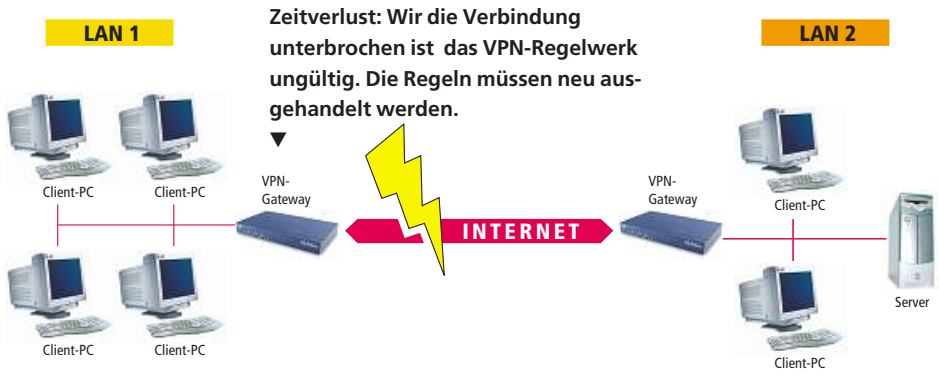
## Anzahl und Art der Selektoren

In der Regel ist nicht jedem Teilnehmer im Netzwerk erlaubt, alle Dienste des Tunnels zu benutzen. Der IPsec-Standard schreibt vor, dass eine Auswahl der zu übertragenden Datenpakete nach IP-Adresse oder IP-Adressrange, -Protokoll und -Port möglich sein muss.

für geschäftskritische Datenströme im Bereich der Warenwirtschafts- oder Kassensysteme gewährleistet ist. Mit Quality of Service kann festgelegt werden, dass beispielsweise 50 Prozent der vorhandenen Bandbreite ausnahmslos für den IPsec-Tunnel reserviert ist, während die anderen 50 Prozent für das Surfen zur Verfügung stehen.

## IPsec braucht Überwachung

Die Nutzung von Quality of Service innerhalb eines IPsec-Tunnels ist vor allem für Unternehmen von Bedeutung, die geschäftskritische Applikationen über einen IPsec-Tunnel




Die Kriterien werden als Selektoren bezeichnet, mit deren Hilfe sich einzelne Dienste für bestimmte Benutzer oder Benutzergruppen sperren lassen.

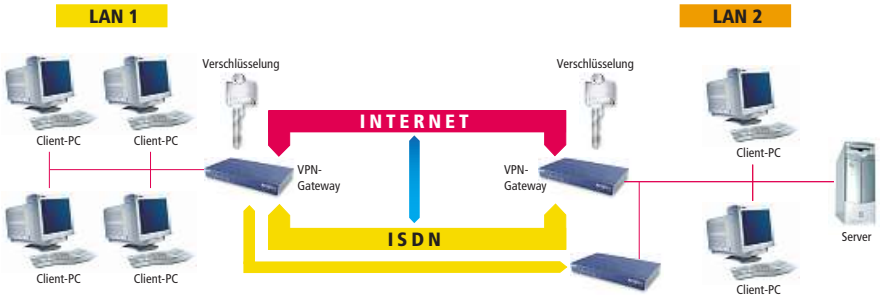
IPsec erlaubt eine sehr komplexe Definition der Anwendungsstrategie. Durch das Selektoren-Konzept sind die Regeln der Anwendungsstrategie, die für eingehende und ausgehende Pakete verwendet werden, zahlreich. Es wird dabei unterschieden zwischen groben Selektoren wie der Netzwerk-Adresse 192.1.1, die alle Computer im gleichen Sub-Netzwerk umfasst, und feinen Selektoren wie der IP-Adresse, die den Arbeitsplatzrechner selbst definiert. Daneben gibt es bestimmte Ports, die nur ein Protokoll (Port 80 für Internet-Zugang über HTTP) bestimmen.

## IPsec und Quality of Service

Leistungsfähige Gateways bieten neben der Selektoren-Auswahl noch die Möglichkeit, sowohl dem IPsec- als auch dem nicht IPsec-basierten Datenverkehr durch Quality-of-Service-Mechanismen unterschiedliche Bandbreiten zuzuweisen. Dadurch lässt sich sicherstellen, dass die notwendige Bandbreite abwickeln und/oder Voice over IP einsetzen.

Das Konfigurieren eines IPsec-Gateways erfordert nach wie vor genaues Fachwissen, will der Administrator sich nicht mit einer Minimal-Implementierung zufrieden geben. So muss der Administrator zwischen verschiedenen Verschlüsselungsverfahren, diversen Berechnungsalgorithmen oder Authentifizierungsverfahren wählen. Bei einfachen Geräten um die 80 bis 100 Euro fehlen diese Auswahlmöglichkeiten. Ärgerlich ist, wenn zwar alles vorschriftsmäßig konfiguriert wurde, aber trotzdem nichts geht. Dies kann unter anderem daran liegen, dass der oder die Tunnel durch die Gateways selbst nicht genügend überwacht werden.

Das Gateway erstellt anhand der durch die Konfiguration vorgegebenen Parameter für jede Verbindung ein Regelwerk. Dies ist die so genannte Security Association (SA), die zuvor mit dem Partner-Gateway ausgehandelt wurde. Im Falle einer einseitigen Unterbrechung der Verbindung wird das Regelwerk ungültig, zum Beispiel durch den Wechsel der IP-Adresse bei dynamischen Adressen oder durch Reboot, Ausschalten, Stromausfall, Leitungsunterbrechung oder Neukonfiguration.




▲ **Wichtig für eine dauerhafte Internet-Verbindung ist ein ISDN-Fall-back, wenn die Standleitung nicht funktioniert.**

Das gilt zumindest für ein Gateway. Das andere bekommt das Löschen des Regelwerks nicht zwangsläufig mit.

Das zweite Gateway geht weiter davon aus, dass die anfangs ausgehandelten Regeln bis zum Ende der Gültigkeit angewandt werden. Die Lebenszeit von Regelwerken beträgt, je nach Sicherheitskonzept des Administrators, zwischen einer und acht Stunden. Je kürzer die Lebenszeit, desto sicherer. Aber umso langsamer wird auch die Verbindung, da die SAs zwischen den IPsec-Gateways ständig neu ausgehandelt werden müssen.

Das erste Gateway schickt verschlüsselte Pakete, weil es davon ausgeht, einen sicheren Tunnel etabliert zu haben. Diese wurden nach dem zuvor ausgehandelten Regelwerk (SA) verschlüsselt. Da das zweite Gateway dieses Regelwerk nicht mehr kennt (die SA wurde gelöscht), werden die eingehenden Pakete verworfen. Professionelle IPsec-Gateways bieten zumindest eine Überwachungsmöglichkeit für die zugrunde liegende physikalische Verbindung wie etwa T-DSL sowie für den IPsec-Tunnel selbst. Für das Letztere hat beispielsweise die Firma Bintec in die IPsec-Gateways die Funktion »IPsec Heartbeat« implementiert. Um festzustellen, ob eine SA noch gültig ist, werden Überwachungspakete (Heartbeats) durch den VPN-Tunnel geschickt. Kommt keine Antwort mehr von der anderen Seite, werden die bestehenden IPsec-Regeln gelöscht und ein neues Regelwerk zwischen den Gateways ausgehandelt.

## ISDN-Backup und Verfügbarkeit

Trotz aller Bemühungen der Hersteller erreichen IPsec-Gateways nicht die gleiche hohe Verfügbarkeit wie traditionelle Festverbindungen. Das Problem liegt häufig im verwendeten Transportmedium selbst: dem Internet. Für alle, die zeitkritische Applikationen über IPsec-Tunnel betreiben möchten, ist daher eine Backup-Möglichkeit verpflichtend. In der Praxis hat sich ein ISDN-Backup bewährt. Wichtig für eine Backup-Lösung ist die Überwachung der IPsec-Verbindung. Des Weiteren sollte der Anwender darauf achten, ob ein ISDN-Modem in das Gateway integriert ist oder extern angeschlossen werden muss. Dies wirkt sich zum einen sehr stark auf die Länge der Zeitspanne aus, bis eine Backup-Verbindung steht und zum anderen auf die Dauer, bis gegebenenfalls wieder auf die DSL-Leitung zurückgeschaltet wird.

Hochwertige IPsec-Gateways integrieren ein ISDN-Modem mit einer automatischen Backup-Umschaltung auf ISDN und Rückschaltung auf X-DSL, sollte diese Verbindung wieder verfügbar sein.

Aus Kostengründen sollte das ISDN-Backup zunächst über die Einwahl zum lokalen Provider stattfinden. Erst wenn das nicht möglich ist, sollte das Gerät versuchen, eine ISDN-Direktverbindung aufzubauen.

Sehr gute IPsec-Gateways bieten darüber hinaus noch weitere Backup-Möglichkeiten. Je nachdem, wo die Störung auftritt, kann ein einfacher ISDN-Backup nicht ausreichen. Eventuell liegt das Problem nicht im Übertragungsweg, sondern im IPsec-Gateway des Partnernetzes. Hier helfen redundant ausgelegte Geräte. Das zweite Gateway übernimmt dabei die Verbindungen vom ausgefallenen.

Liegt das Problem allerdings nicht im VPN-Gateway, sondern im Zugangs-Netzwerk des Providers, sollte das lokale VPN-Gateway in der Lage sein, ein zweites Gateway im Partner-Netzwerk anzusteuern. Dieses alternative IPsec-Gateway ist dann über einen zweiten Provider angebunden. Die Verbindung kann so in jedem Fall aufrechterhalten werden, außer es werden im Rahmen von Bauarbeiten die physikalischen Leitungen gekappt.

Um dieses Problem zu umgehen, gibt es gegenwärtig keine funktionierenden Angebote auf dem Markt. Das könnte sich jedoch bald ändern, wenn Backups über schnelle UMTS-Verbindungen möglich sind. BBR

# Linux-Spam-Filter

**Ein Linux-Server und das Open-Source-Programm Spam Assassin schützen das lokale Netzwerk wirkungsvoll vor unerwünschter Werbepost.**

Martin Goldmann

Firmen und kleine Betriebe verwalten oft ihre E-Mails mit POP- oder IMAP-Servern unter Linux. Von den Servern holen die E-Mail-Clients der Mitarbeiter neue Nachrichten ab. Und mit diesen kommt eine lästige Fracht: unerwünschter Werbemüll. Die Lösung des Spam-Problems wird umso dringender, je größer ein Unternehmen ist. Die Nachrichtenflut blockiert Server und Datenleitungen. Und die Mitarbeiter verlieren viel Zeit, um die für sie relevanten Mails von Werbemüll zu trennen. Der Netzwerk-Administrator muss also die unerwünschten Mails so früh wie möglich stoppen.

Ein geeigneter Angriffspunkt gegen Spam sind die Postfächer der Mitarbeiter. Die liegen in Unternehmen auf einem Linux-Server, ein Mail-Transport-Agent legt die eingehenden Nachrichten in den Postfächern ab. Und genau hier greift die Spam-Abwehr. Diese sortiert die Spam-Nachrichten aus und lässt nur relevante Mails durch die Filter passieren.

## Spam Assassin installieren

Als Betriebssystem dient im folgenden Beispiel Suse Linux 9.0. In der Distribution ist eine aktuelle Version des Programms Spam Assassin enthalten. Um die Anti-Spam-Software zu installieren, starten Sie *Yast* und wählen *Suche nach Paketen*. Geben Sie als Suchbegriff *spam* ein. In den Suchergebnissen findet sich das Paket *spamassassin*. Nach dessen Installation öffnet der Netzwerk-Administrator eine Shell mit Root-Zugriffsrechten. Der Befehl *insserv spamd* installiert den Spam-Assassin-Dämon so, dass dieser beim nächsten Systemstart mit geladen wird. Um den Dämon zusätzlich auch gleich zu starten, muss *rcspamd start* eingegeben werden.

Die nächsten Arbeiten betreffen den Mail-Agent Postfix. Den muss der Anwender anweisen, alle eintreffenden Mails mit Procmail weiterzuverarbeiten. Denn genau dort klinkt sich Spam Assassin in das System ein.

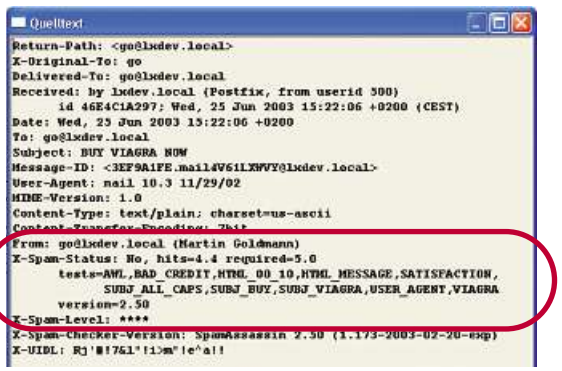
Dafür öffnet der Anwender die Datei */etc/sysconfig/postfix* und trägt dort beim Parameter *POSTFIX_MDA* als Wert procmail ein: *POSTFIX_MDA=procmail*.

Sind die Änderungen erledigt, geht es auf der Kommandozeile weiter mit der Eingabe des Befehls *SuSEconfig*. Anschließend werden die Konfigurationsdateien neu geschrieben. Nach der Eingabe von *rcpostfix restart* startet der Mail-Server automatisch neu.

Jetzt braucht das Home-Verzeichnis jedes Mail-Users eine neue *.procmailrc*. Eine solche, bereits vorbereitete Datei findet sich im Verzeichnis */usr/share/doc/packages/perl-spamassassin*. Falls in einem Heimatverzeichnis bereits eine *.procmailrc* vorhanden ist, sichern Sie diese zunächst mit *cp/home/user/.procmailrc/home/user/procmailrc.bak*. An Stelle von *user* muss der jeweilige Benutzername stehen.

Anschließend kopiert der User die vorbereitete *.procmailrc* aus dem Verzeichnis: *cp /usr/share/doc/packages/perl-spamassassin/procmailrc.examplehome/user/.procmailrc*.

Das Sichern und Kopieren muss für jeden Benutzer ausgeführt werden, der ein Mail-Postfach auf dem Server hat. Für den Anfang sollte diese Aktion auf einen Testnutzer beschränkt bleiben. Im Grunde ist die Konfigu-




▲ **Nach dem Installieren von Spam Assassin erhält jede einzelne ankommende E-Mail eine Spam-Kennzeichnung und -Bewertung im E-Mail-Header.**

ration jetzt einsatzbereit. Treffen mehrere Mails gleichzeitig auf dem Server ein, wird diese Konfiguration zu langsam. In diesem Fall muss in der Datei *.procmailrc* im Bereich

```
:0fw: spamassassin.lock
* < 256000
| spamassassin
```

die Zeile

```
| spamassassin
```

geändert werden in

```
| spamc
```

Mit diesen Einstellungen wird jede eintreffende E-Mail an *spamc* weitergeleitet. Das ist das entsprechende Client-Programm des in C programmierten Dämons *spamd*. Diese Kombination arbeitet schneller als der Aufruf *spamassassin*.

### Der erste Test mit Spam Assassin

Gehen Sie gewissenhaft nochmals folgende Checkliste durch:

- *Postfix* so umkonfiguriert, dass Procmail Mails verarbeitet
- *SuSEconfig* und Neustart von Postfix ausgeführt
- *spamd* mit *insserv* eingetragen
- *spamd* gestartet
- *procmailrc* in Benutzerordner kopiert
- *spamc* in *.procmailrc* eingetragen

Sind alle Einträge abgehakt, meldet sich der Netzwerk-Administrator mit einem beliebigen Benutzernamen an, in dessen Home-Verzeichnis zuvor eine *.procmailrc* kopiert wurde. Dieser Testanwender schreibt von der Kommandozeile aus eine E-Mail an sich selbst, indem er *mail user* eingibt und anschließend [Return] drückt. An Stelle des Platzhalters *user* muss der Anwender den entsprechende Benutzernamen eintragen.

In der Mail dürfen ein gängiger Betreff und ein beliebiger Inhalt stehen. Das bedeutet: lesbar und nicht Spam-verdächtig. Mit der Tastenkombination [Strg D] geht die Mail auf die kurze Reise in das eigene Postfach.

Mit der Eingabe von *mail* erscheint der Posteingang des Benutzers auf dem Arbeitsplatzbildschirm. Geben Sie die entsprechende Nummer der E-Mail ein (bei einem noch nicht benutzten E-Mail-Postfach ist das die 1). Anschließend ist die E-Mail inklusive aller Header zu sehen, zum Beispiel:
Message 1:

```
From go@lxdev.local  Wed Jun 25 14:12:58 2003
X-Original-To: go
Delivered-To: go@lxdev.local

Date: Wed, 25 Jun 2003 14:12:58 +0200
To: go@lxdev.local
Subject: Testmail
User-Agent: nail 10.3 11/29/02
MIME-Version: 1.0
Content-Type: text/plain; charset=iso-8859-1
Content-Transfer-Encoding: 8bit
From: go@lxdev.local (Martin Goldmann)

X-Spam-Status: No, hits=0.0 required=5.0
       tests=USER_AGENT
       version=2.50
X-Spam-Level:
X-Spam-Checker-Version: SpamAssassin 2.50
(1.173-2003-02-20-exp)

Das ist eine Testmail. Sie prüft, ob die Spamab-
wehr aktiv ist.
```

## So funktioniert Spam Assassin

Beim Einsatz des von Suse-Linux kostenlos mitgelieferten Spam Assassin muss der User einiges beachten. Spam Assassin erhält vom Mail-Transport-Agent (MTA), meist Postfix oder Sendmail, jede eingehende E-Mail. Dieser scannt die Mails anhand vieler für Spam-Nachrichten typischer Kriterien. Spam Assassin überprüft etwa, ob im Absender neben der Adresse auch ein echter Name steht, ob in der Mail eine oder mehrere Namen durchgehend in Großschrift geschrieben sind oder wann die Mail verschickt wurde. Außerdem testet die Software, zu wie viel Prozent die Mail aus HTML-Code besteht. Auch typische Spam-Phrasen wie »Money back guarantee« oder «Free offer« gehen dem Spam Assassin ins Netz. Jedes der Kriterien hat einen Punktwert. Trifft ein Kriterium zu, geht dieser Wert in die Gesamtwertung ein. Überschreitet die Gesamtwertung einen voreingestellten Punktwert, markiert Spam Assassin die Nachricht als Spam und leitet diese wieder an den MTA oder an eine Ablage für Spam-Mail weiter. Dieses heuristische Verfahren hat einen Vorteil: Es erkennt viele verschiedene Arten von Spam-Mail. Auch solche, die bislang noch nicht im Umlauf waren. Nachteil der Heuristik: In manchen Fällen liegt der Spam-Filter daneben und erzeugt »false positives«, also fälschlich als Spam markierte Nachrichten. Aus diesem Grund ist es wichtig, Spam-Mail nicht zu löschen, sondern auf dem Server in einer Art Quarantäne-Datei aufzubewahren. Stellt sich dann heraus, dass ein Benutzer eine Nachricht vermisst, kann der Administrator diese wiederherstellen.

Wer Spam Assassin im LAN einsetzt, sollte zusätzlich den Razor-Agent verwenden. Erkennt der Spam-Filter eine neue Junk-Mail, bildet das Tool aus dem Mail-Inhalt eine eindeutige Prüfsumme. Diese leitet die Software an den Razor-Server weiter. Anhand der Signatur können andere Spam-Vermeidungs-Programme Junk-Mail erkennen und ausschließen. Die Datenbank wächst so mit jeder neu auftretenden Spam-Mail und wirkt damit effektiv gegen neuen Spam. Der Razor-Agent befindet sich in Suse-Linux, mehr Informationen erhalten Anwender unter der Adresse *razor.sourceforge.net*.

Entscheidend sind X-Spam-Status und -Level. Der X-Spam-Status dient als Protokoll und zeigt, welche Punktzahl die E-Mail bei den Spam-Tests erreicht hat. Der Spam-Level zeigt eines oder mehrere Sternchen, die Aufschluss über die Spam-Wahrscheinlichkeit geben. In diesem Fall ist die Spam-Wahrscheinlichkeit gleich Null, also gibt es auch kein Sternchen.

## Den Mail-Reader verlassen

Ein zweiter Versuch: Um den Mail-Reader zu verlassen, gibt der System-Administrator zweimal *q* ein. Danach folgt wieder die Eingabe von *mail user*.

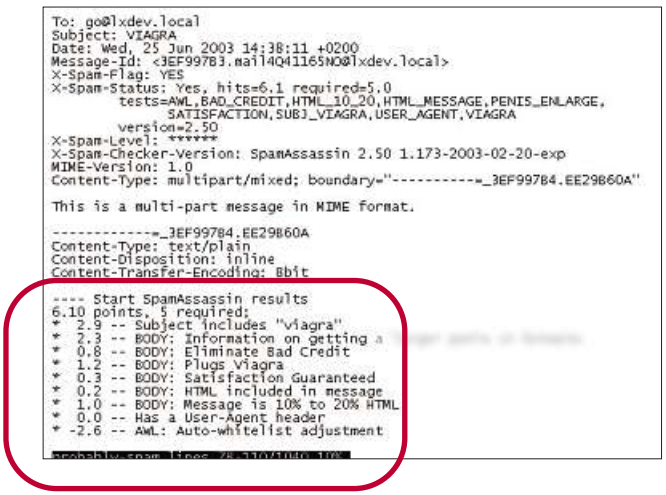
Als Titelzeile dient der aktuelle Spam-Renner schlechthin:

```
BUY VIAGRA NOW
Im Mail-Text geht es weiter mit:
<h1>NO DEBT ANYMORE
SATISFACTION GUARANTEED
NO CREDIT CARD REQUIRED</h1>
```

Das sind typische Spam-Phrasen, eingebettet in ein HTML-Tag. Nach dem Versenden der Mail erscheint folgende Meldung:

```
X-Spam-Status: No, hits=4.4 required=5.0
tests=AWL,BAD_CREDIT,HTML_00_10,HTML_MESSAGE,
SATISFACTION,
SUBJ_ALL_CAPS,SUBJ_BUY,SUBJ_VIAGRA,USER_AGENT,
VIAGRA
version=2.50
X-Spam-Level: ****
```

Diese Mail hat es noch durch den Filter geschafft. Hinter *tests* stehen alle Kriterien, die für die Bewertung der Mail zutreffen. »HTML_00_10« deutet an, dass bis zu zehn Prozent HTML enthalten sind, »HTML_MESSAGE« bedeutet, dass es sich um eine in HTML verfasste Nachricht handelt. Die mit »SUBJ« beginnenden Einträge zeigen, dass die Betreffzeile in Großbuchstaben geschrieben ist und dass es sich um eine Kaufaufforderung für Viagra handelt. Das sind genug Indizien, um die Mail umgehend in den Papierkorb zu verschieben. Doch der Eintrag *AWL* rettet die Mail. *AWL* steht für Automatic Whitelist. Diese Datei registriert sämtliche Absender, die eine Mail an den Benutzer schicken. Für jede Spam-freie Mail gibt es einen Bonus, für jede Junk-Mail einen Malus. Nachdem zuvor in diesem Beispiel eine saubere Mail vom selben Absender verschickt wurde, bekommt dieser nun einen positiven Wert in der Whitelist.




**Gefiltert: Diese Mail erreichte 6,1 Spam-Punkte und wird damit als Spam aussortiert.**

Mit ein paar Spam-E-Mails mehr lässt sich dieser Wert aber zu Ungunsten des Absenders verändern. Hierfür erzeugt der Administrator eine Textdatei *spam.txt* mit dem Inhalt:

```
<h1>BUY NOW
USE VIAGRA
NO DEBT
SATISFACTION GUARANTEED</h1>
```

Nach dem Speichern versendet nachfolgender Befehl die Mail an den Benutzer »user«.

```
cat spam.txt | mail user -s "VIAGRA"
```

Dieser Befehl lässt sich nach einem Tastendruck auf [Pfeil oben] beliebig oft wiederholen. Aber schon nach dem ersten Mal sollte die Mail im Junk-Filter hängen bleiben. Ein Blick in die Datei *probably-spam* im Heimatverzeichnis des Nutzers bestätigt das. Hier findet sich die Mail mit den Informationen, warum diese als Spam gekennzeichnet wurde:

```
-- Start SpamAssassin results
5.40 points, 5 required;
*  2.9 - Subject includes "viagra"
*  0.8 - BODY: Eliminate Bad Credit
*  1.2 - BODY: Plugs Viagra
*  0.3 - BODY: Satisfaction Guaranteed
*  0.2 - BODY: HTML included in message
*  1.0 - BODY: Message is 10% to 20% HTML
*  0.0 - Has a User-Agent header
* -1.0 - AWL: Auto-whitelist adjustment
-- End of SpamAssassin results
```

2,9 Punkte gab es für »viagra«, 0,3 für garantierte Zufriedenheit und einen weiteren für HTML. Wichtig ist die unterste Zeile: Die Zeile zieht einen Bonuspunkt ab, da der Ab-

| AREA TESTED | LOCALE | DESCRIPTION OF TEST | TEST NAME | SCORES (local, net, with bayes, with bayes+net) |
|---|---|---|---|---|
| header | | Message-Id indicates a non-spam MUA (Pine) | USER_AGENT_PINE | 0.001 |
| header | | User-Agent header indicates a non-spam MUA (Mozilla) | USER_AGENT_MOZILLA_UA | -0.498 0.001 -0.498 0.001 |
| header | | X-Mailer header indicates a non-spam MUA (Netscape) | USER_AGENT_MOZILLA_XM | 0.001 |
| header | | User-Agent header indicates a non-spam MUA (Outlook Express) | USER_AGENT_MACOE | 0.001 |
| header | | User-Agent header indicates a non-spam MUA (Entourage) | USER_AGENT_ENTOURAGE | 0.001 |
| header | | User-Agent header indicates a non-spam MUA (KMail) | USER_AGENT_KMAIL | -0.399 0.001 -0.299 -0.470 |
| header | | User-Agent header indicates a non-spam MUA (IMP) | USER_AGENT_IMP | 0.001 |
| header | | X-Mailer header indicates a non-spam MUA (T-Offline) | USER_AGENT_TONLINE | -0.425 -0.499 -0.189 -0.349 |
| header | | X-Mailer header indicates a non-spam MUA (Apple Mail) | USER_AGENT_APPLEMAIL | 0.001 |
| header | | User-Agent header indicates a non-spam MUA (Gnus) | USER_AGENT_GNUS_UA | -0.480 -0.499 -0.499 -0.480 |

**◀ Auf der Homepage von Spam Assassin (www.spamassasin.org) findet sich eine Liste der überprüften Eigenschaften einer Mail.**

sender schon eine saubere Mail geschickt hatte. Der Abzug wird sich mit jeder weiteren Spam-Mail verringern. Nach einem zweiten Versand derselben Mail steht dieser Wert in diesem Beispiel nur noch bei -0,7 und wird sich schließlich in einen Aufschlag verwandeln. Eine komplette Liste der Tests, der dabei vergebenen Punkte und der Schlüsselwörter erhalten Anwender unter *spamassassin.org/tests.html*.

## Feintuning für Anwender

Falls ein Benutzer über entsprechende Rechte verfügt, kann er eigene Einstellungen vornehmen. Dazu öffnet der User innerhalb seines Heimatverzeichnisses den Ordner *.spamassassin* und darin die Datei *user_prefs*. Wichtig ist der Eintrag *blacklist_from*. Hier lassen sich Mail-Adressen oder Teile davon blockieren. Ein Beispiel: *blacklist_from *@foo.bar blockiert* alle Mails, bei denen in der *Absenderadresse@foo.bar* steht.

Ebenso lassen sich mit *whitelist_from* vertrauenswürdige Absender und Domains festlegen, beispielsweise mit *whitelist_from musteruser@foo.bar*.

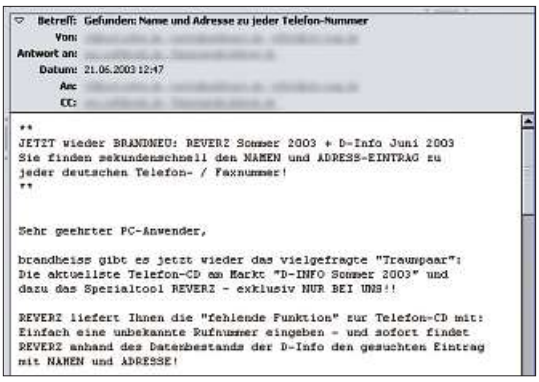
Ein weiteres, interessantes Einsatzgebiet für *user_prefs* ist die Gewichtung einzelner Kriterien. Ein Arzt oder Apotheker mag die entsprechenden Spam-Kriterien niedriger ansetzen. Dies erledigt er etwa mit dem Eintrag *score SUBJ_VIAGRA 0* in *user_prefs*. Damit wird das Vorkommen von »viagra« in der Betreffzeile nicht mehr negativ bewertet.

Ebenso wie für jeden einzelnen Benutzer lassen sich systemweit Richtlinien vergeben. Die stehen in der Datei */etc/mail/spamassassin/local.cf*. Ein gerade für größere Server wichtiger Eintrag ist *required_hits*. Damit passt der Systemadministrator den Wert an, ab dem eine Mail als Spam gekennzeichnet wird. Je mehr Benutzer der Mail-Server verwaltet, desto großzügiger sollte dieser Wert gesetzt werden. Der Standardwert liegt bei 5.0, für das Erste kann man ihn auf 8.0 erhöhen. Das funktioniert mit dem Eintrag *required_hits 8.0*. Weitere Parameter finden Sie mit *perldoc Mail::SpamAssassin::Conf*.

Falls sich die Dokumentation vom Root-Account aus nicht aufrufen lässt, meldet sich der Netzwerk-Administrator mit einem beliebigen Benutzernamen an. Bequemer ist die Konfigurationsübersicht jedoch über das Internet zu erreichen: *spamassassin.org/doc/Mail_SpamAssassin_Conf.html*

## Fazit

Es empfiehlt sich, den Spam-Filter erst einmal mit einigen Test-Accounts auszutesten und dann die Feineinstellungen anzupassen. Denn der Spam-Filter muss den Kompromiss schaffen zwischen möglichst effektiver Spam-Abwehr und möglichst wenigen »false positive« eingestuften Mails. BBR




**▲ Deutschsprachiger Spam aus der Schweiz verfängt sich nicht so schnell im Netz von Spam Assassin. Hier hilft die Blacklist oder das Erzeugen eigener Regeln.**

# 7 Vollversionen

**Mit dem großen Sicherheitspaket auf der Heft-CD schützen Sie sich gezielt vor Viren, Trojanern und Spyware sowie Hacker-Attacken aus dem Internet.**

Christoph Hoffmann

Die beiden für den privaten Einsatz kostenlosen Programme AntiVir Personal Edition 6.23 und AVG AntiVirus 6.0 Free Edition schützen Windows-PCs vor Viren. Dabei werden alle Windows-Aktivitäten überwacht und Dateien direkt beim Öffnen oder Ausführen geprüft. Unter dem Einsatz modernster Technologien wie etwa einer heuristischen Analyse werden sogar unbekannte Viren erkannt. Dank Online-Update lassen sich die Programme aktuell halten.

Mithilfe von Filterregeln legen Sie in der Sygate Personal Firewall 5.5 Standard fest, welche Programme eine Online-Verbindung aufnehmen dürfen und welche nicht. Die Statistikfunktionen geben Aufschluss über aktive Internet-Verbindungen. Nach der Installation ist die Desktop-Firewall aktiv und blockiert standardmäßig jede Online-Verbindung. Erst nach der Freigabe des Anwenders wird diese hergestellt.

Viele Free- und Shareware-Programme installieren ungefragt Spyware-Komponenten auf dem Windows-PC. Ein Virenscanner bietet nur unzureichenden Schutz. Besser arbeitet das Tool Pest-Patrol Express, das vor Spy- und Malware schützt.

GhostSurf Express 2.0 verwischt Ihre verräterischen Spuren im Internet und lässt Sie anonym surfen. Eine Rückverfolgung ist dann nicht mehr möglich. Im *Ghost Mode* kontrolliert die Software interaktiv Cookies, Temporärdateien, Proxyserver, History-Files, IP-Adressen und Host-Server.

Zone Alarm 4.5 ist eine Personal-Firewall zum Schutz gegen Hacker und das Ausspähen vertraulicher Daten. Die neue Benutzeroberfläche macht den Einstieg noch

## CD-Inhalt

### Vollversionen

| | |
|---|---|
| Antivir Personal Edition 6 | Vollversion |
| AVG AntiVirus 6.0 FE | Vollversion |
| GhostSurf 2.0 Express | Vollversion |
| PestPatrol Express | Vollversion |
| Sygate Firewall 5.5 Std. | Vollversion |
| VersionBackup 2.10 | Vollversion |
| ZoneAlarm 4.5 | Vollversion |

### Virenscanner

| | |
|---|---|
| Antivir Professional 6.22 | Testversion |
| AVG Professional 7 Single Edition | Testversion |
| Antiviren Kit 2004 Professionell | Testversion |
| BitDefender Standard 7.2 | Testversion |
| Bullguard 3.5 | Testversion |
| F-Secure Anti-Virus 2004 | Testversion |
| Norman Virus Control 5.7 | Testversion |
| Panda Antivirus Platinum 7 | Testversion |
| Panda Antivirus Titanium 2 | Testversion |
| PC-Cillin 11 | Testversion |
| Tauscan 1.65 | Testversion |
| The Cleaner 4.0 Professional | Testversion |

### Desktop-Firewalls

| | |
|---|---|
| 8Signs Firewall 2.08 | Testversion |
| F-Secure Internet Security 2004 | Testversion |
| HackerSmacker 1.1 | Testversion |
| Kaspersky Anti-Hacker 1.5 | Testversion |
| Kerio Personal Firewall 4 | Testversion |
| Norman Personal Firewall 1.4 | Testversion |
| Norton Personal Firewall 2004 | Testversion |
| Outpost Personal Firewall 2.0 Pro | Testversion |
| PC-Cillin Internet Security 11 | Testversion |
| Sygate Personal Firewall 5.5 Pro | Testversion |
| TermiNET Personal Firewall | Testversion |
| ZoneAlarm Pro 4.5 | Testversion |

### Anti-Spam-Tools

| | |
|---|---|
| SpamPal 1.53 | kostenlos |
| Spamihaliator 0.9.7.2 | kostenlos |
| SpamEater Pro 3.65 | Testversion |
| SuperSpamKiller Pro 3.15 | Testversion |
| PacSpam Pro 6.4.1 | Testversion |
| Simons Spamkiller 1.40 | Testversion |
| AntiSpamWare 2.0 | Testversion |
| SpamNet 2.3.4 | Testversion |

### Security-Tools

| | |
|---|---|
| 0190/0900 Warner 4.01 | kostenlos |
| Ad-Aware Standard 6 | kostenlos |
| JAP Anonymity & Privacy | kostenlos |
| SpyBot Search & Destroy 1.2 | kostenlos |
| PestPatrol 4.3 | Testversion |
| GhostSurf 3.0 Premium | Testversion |
| Spy Sweeper 2.2 | Testversion |
| WebWasher 3.3 Classic | kostenlos |
| ArchiCrypt Stealth 2.7.1 | Testversion |
| Hacker-Eliminator 1.2 | Testversion |
| Ethereal Network Analyzer 0.91 | kostenlos |
| CommView 4.0 | Testversion |
| SuperScan 4.0 | kostenlos |
| Secure IT Pro 4.70 | kostenlos |
| WinGuard Pro 2004 5.6.17 | kostenlos |
| EasyCrypto Deluxe 5.5 | kostenlos |
| DriveCrypt 4.0 | Testversion |
| Process Explorer 8.1 | kostenlos |

### Internet-Browser

| | |
|---|---|
| Abolimba Multibrowser 3.0 | Shareware |
| Avant Browser 8.02 | kostenlos |
| DX-Browser 4.0 | kostenlos |
| Firebird 0.7 | kostenlos |
| Internet Explorer 6.0 SP1 | kostenlos |
| Mozilla 1.5 | kostenlos |
| Multibrowser 7.05 | Shareware |
| NetCaptor 7.5 PE | kostenlos |
| Netscape 7.1 | kostenlos |
| Opera 7.22/ 7.23 | kostenlos |

### Windows-Basics

| | |
|---|---|
| Adobe Reader 6.01 | kostenlos |
| VB-Runtimes | kostenlos |
| MS-Installer 2.0 | kostenlos |
| Java Runtime 1.42 | kostenlos |
| WinZip 8.1 | Shareware |
| WinRAR 3.20 | Shareware |
| WinAce 2.50 | Shareware |
| PowerArchiver 8.6 | Shareware |
| UltimateZip 2.7.1 | kostenlos |
| ZipGenius 5.5 Suite | kostenlos |

## Hinweise zur Heft-CD

Bitte beachten Sie, dass weder die Redaktion *PC Professionell* noch die Stroemung GmbH Support zu den Programmen auf der Heft-CD leisten können. Bei Fragen zu einer Software wenden Sie sich direkt an den Hersteller. Die Weblinks finden Sie auf der Heft-CD.
Bei sonstigen Problemen mit der Heft-CD ist die *PC-Professionell*-Redaktion per E-Mail an die Adresse *leserbrief@pc-professionell.de* erreichbar. Sollte die CD-ROM zu dieser Ausgabe fehlen oder defekt sein, kann sie beim Leser-Service unter der Telefonnummer (0711) 725 22 99 nachgefordert werden.

Das Herunterladen und die Installation der auf der Heft-CD bereitgestellten Software erfolgen auf eigene Gefahr. VNU Business Publications Deutschland übernimmt keine Gewährleistung oder Haftung für die Funktionsfähigkeit und etwaige Schäden, die durch die Installation entstehen können.

Die Heft-CDs werden vor der Produktion mit Norton Antivirus 2004, Tauscan 1.6 und The Cleaner 4.0 Professional auf Viren und Trojaner untersucht. Sollte es zu einem Virenalarm kommen, setzen Sie sich mit dem Hersteller Ihrer Antiviren-Software in Verbindung.

einfacher. Ein integriertes Modul ermöglicht Filtern, Sortieren und Echtzeitanalyse der protokollierten Daten. Das mehrstufige Schutzsystem schirmt PCs vor ein- und ausgehenden Bedrohungen ab. Der MailSafe-Schutz stoppt per E-Mail übertragene VBS-Viren.

### Aktion: Version-Backup 2.10

Typische Backup-Programme ermöglichen die Rekonstruktion des Stands vom Vortag, eine Historie für ältere Sicherungen bieten aber meist nur hochpreisige Lösungen. Für Komfort und Übersicht sorgt das Backup-Archivsystem Version-Backup. Hiermit können Sie nicht nur den Stand des Vortages wieder herstellen, sondern auch den Stand eines beliebigen früheren Tages. Die Backups bleiben so lange verfügbar, wie Sie es wünschen.Version-Backup verwendet eine Kombination aus inkrementellen Backups und Voll-Backups. Die Vollversion erlaubt das Zwischenspeichern beliebig vieler Datensicherungen und ist für Stand-alone-PCs optimiert. Einmal täglich wird automatisch von den gewünschten Verzeichnissen eine Sicherung erstellt. Im Gegensatz zu den reinen Backup-Kopierprogrammen werden dabei frühere Sicherungsstände nicht überschrieben. Wenn Sie Dateien oder Verzeichnisse wiederherstellen möchten, wird eine Datumsliste der vorhandenen Stände angezeigt. Nach der Auswahl des Datums rekonstruiert das Programm den Stand exakt von diesem Tag. Die netzwerktaugliche Ausführung Version-Backup Master mit zusätzlichen Funktionen kostet regulär 48 Euro und ist über den Link auf der Heft-CD bis zum 30. Mai 2004 zum Sonderpreis von 39 Euro mit der Bonus-Codenummer 2564-8212-0148 erhältlich. Mit der Master-Version kann die Sicherung über das Netzwerk direkt zu einem anderen Computer erfolgen. Außerdem lassen sich Backup-Versionen auslagern, zum Beispiel auf CD. Die externen Datenträger sind in die Recovery-Funktion eingebunden.

