COMPUTERWÜRMER

Die Virenflut und ihre Opfer

Seit ein paar Monaten vermehren sich Computerwürmer so rasant, dass sie früher oder später jedes Postfach erreichen, so etwa geschehen bei MyDoom.A (siehe unten rechts). Eine derart massive Wurmverbreitung kommt nur zu Stande, weil noch zu viele Benutzer immer wieder die wichtigste Sicherheitsregel missachten: Keine unbekannten Mailbeilagen öffnen! Die Rechnung dafür bezahlt einerseits der unvorsichtige Benutzer. Nicht nur, weil er durch den Wurmbefall vielleicht wichtige Dateien verliert, sondern auch, weil viele Computerwürmer auf dem PC eine Hintertüre installieren. Diese erlaubt es einem Angreifer, persönliche Informationen (Passwörter, Kreditkartendaten) auszuschnüffeln oder den PC zum Versenden von Spammails zu missbrauchen.

Unter der Virenflut haben nicht nur die Besitzer infizierter PCs zu leiden. Die Systemverantwortlichen bei Firmen und Internetprovidern klagen allesamt über höhere Ausgaben, um die Infrastruktur der steigenden Mailflut anzupassen. Grössere Festplatten und teure Filter- und Antiviren-Software sind nur zwei der grossen Posten. Sogar wer sein System sauber hält, muss jetzt nicht nur täglich noch mehr Spam, sondern auch unzählige Exemplare der aktuell kursierenden Schädlinge aus seinem Postfach räumen, allen voran die Würmer Swen (mehr dazu in WEBCODE **25198**) und Dumaru.Y (WEBCODE **26369**).

Sie sollten Ihren PC einer eingehenden Prüfung unterziehen. Beseitigungswerkzeuge gibts im Netz: Sowohl McAfees «Stinger» (http://vil.nai.com/vil/stinger) als auch «Clrav» von Kaspersky (www.kaspersky.com/de/news.html?id=3112351) helfen weiter. (*sal*)

KURZINFOS

LÖCHRIG

In mehreren Versionen des RealOne Players sind Schwachstellen entdeckt worden. Ein Patch ist über die Aktualisierungsfunktion des RealOne Players verfügbar.

TÄUSCHUNG

Der US-Branchendienst Cnet warnt vor schwarzen Schafen unter den Anti-Spyware-Anbietern. So soll etwa das Tool SpyBan heimlich Benutzerdaten sammeln. Anwendern wird empfohlen, Programme von bekannten und seriösen Anti-Spyware-Firmen wie Lavasoft und Spybot zu verwenden.

WLAN

Die Wi-Fi Alliance plant für dieses Jahr eine neue Version des einjährigen WLAN-Sicherheitsstandards WPA (Wi-Fi Protected Access). Er soll weitere Sicherheitsfunktionen für drahtlose Netzwerke bringen und ab Mitte 2004 unterstützt werden.

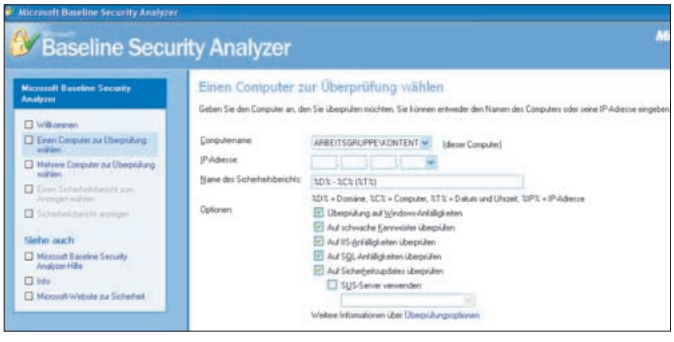
APPLE-PATCH

Für Anwender der Mac-OS-Versionen 10.1.5, 10.2.8 und 10.3.2 steht ein neues Sicherheits-Update zum Download bereit. Es kann über die automatische Software-Aktualisierung heruntergeladen werden.

TOOLS

Ein Wachmann von Microsoft

Microsoft hat die Version 1.2 seines Gratis-Sicherheitstools Microsoft Baseline Security Analyzer veröffentlicht. Es ist im Download-Bereich des PCtipp mit dem WEBCODE **26341** zu finden. Die Software testet Rechner auf fehlende Sicherheits-Updates und andere Schwachstellen. Die neue Version führt umfassendere Tests durch, durchsucht mehr Microsoft-Produkte und ist jetzt auch in Deutsch erhältlich. Nach dem Scan erteilt die Software Ratschläge, wie sich die Lücken beheben lassen.



Der Baseline Security Analyzer testet Ihren Rechner auf Schwachstellen

MICROSOFT-GUIDES

Sicherheits-Tipps vom Hersteller

Microsoft hat zwei Security Guides für Windows XP und Windows 2003 Server ins Download-Center (www.microsoft.com/downloads) gestellt. Die nur in englischer Sprache erhältlichen Dokumente geben Auskunft über die sichere Konfiguration der beiden Betriebssysteme in verschiedenen Arbeitsumgebungen. Sie finden die beiden in einer .exe-Datei steckenden Referenzwerke, wenn Sie im Download-Center nach «Security Guide» suchen.

WURM

Gestoppt, aber nicht gelöscht

Von Ende Januar bis Mitte Februar gelang der A-Variante des MyDoom-Wurms eine so starke Verbreitung, dass er die «Virenhitparaden» aller Antiviren-Hersteller anführte. Wie verschiedene Sicherheitsexperten bei der Analyse des Schädlings herausfanden, war der Wurm dazu programmiert, am 12. Februar seine Verbreitung per E-Mail zu beenden. Wenn dieses Heft erscheint, sollten also keine MyDoom.A-Exemplare mehr verschickt werden.

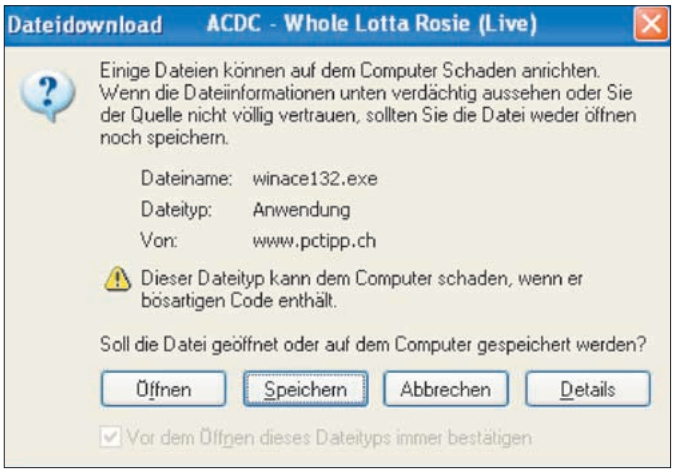
Dass die Verbreitung aufgehört hat, bedeutet aber längst nicht, dass nicht immer noch zehntausende Computer mit diesem Wurm befallen sind. Weil der Wurm einen infizierten PC durch eine Hintertüre angreifbar macht (siehe oben «Die Virenflut und ihre Opfer»), wird nach wie vor empfohlen, ihn vom PC zu entfernen. Informationen und Links dazu finden Sie im PCtipp-Virenticker unter WEBCODE **26385**.

ILLUSTRATIONEN TAVIS COBURN, JOE ZEFF, JACK GALLAGHER, HARRY CAMPBELL, JOHN CUENO

INTERNET EXPLORER

Verräterische Download-Option

Die Sicherheitsfirma Secunia warnt vor einer Sicherheitslücke, die sich beim Download von Dateien auswirkt. Wer eine Datei anklickt, hat normalerweise die Wahl: Sie direkt zu öffnen oder zuerst abzuspeichern. Durch den Fehler ist es nun aber etwa möglich, dass sich beim unverzüglichen Öffnen vom Server hinter einer vermeintlichen PDF-Datei ein ganz anderes Programm verbirgt. Das können Hacker für ihre eigenen bösartigen Zwecke nutzen. Bis Microsoft eine Lösung veröffentlicht, empfehlen Sicherheitsfachleute, Dateien aus dem Internet nie direkt zu öffnen, sondern zuerst in einen Ordner auf der Festplatte zu speichern und auf Viren zu scannen.



Speichern Sie Download-Dateien immer, meiden Sie den Button Öffnen

INTERNET EXPLORER

Patch as Patch can

Mit einem neuen Sammel-Patch, der mehrere Fehler auf einen Schlag beseitigt, räumt Microsoft auch mit der viel kritisierten Spoofing-Anfälligkeit des Internet Explorers auf, der bisher Adressen nach dem Muster www.beispiel.ch%01@www.betrug.ch auf die scheinbar harmlose Site www.beispiel.ch reduzierte. Damit ist jetzt Schluss: Der neue Patch, zu finden via Microsoft Sicherheitsbulletin MS04-004 (www.microsoft.com/germany/ms/technetservicedesk/bulletin), stellt dieses Verhalten ab. Kurz danach hat Microsoft ein Korrektur-Programm veröffentlicht, das einen Fehler in eben diesem Sammel-Patch behebt. Nach der Installation funktionieren bestimmte XML-Aufrufe von Webadressen nicht mehr richtig, bei denen Benutzername und Kennwort eingebunden sind. Stattdessen erscheint die Meldung «Invalid Syntax Error».

DOOMJUICE

Folgeschaden

Was Sicherheitsexperten befürchtet haben, ist eingetroffen. Mit Doomjuice taucht ein weiterer Schädling auf, der die Hintertür ausnützt, die vom MyDoom-Wurm geöffnet wird (siehe auch «Der Wurm zum Wurm», rechts). Der Netzwerkwurm verbreitet sich nicht per E-Mail, sondern klappert das Internet nach Rechnern ab, deren Port 3127 geöffnet ist. Wird er fündig, schleicht er sich automatisch ins System ein. Wie MyDoom.B enthält auch Doomjuice eine Schadensroutine, welche die Microsoft-Website mit einer Attacke in die Knie zwingen will. Weitere Infos zu Doomjuice und dessen Beseitigung finden Sie im aktuellen PCtipp-Virenticker unter WEBCODE **26510**.

VIREN

Der Wurm zum Wurm

Deadhat nutzt die trojanische Software, die von MyDoom installiert wird. Auf befallenen Systemen versucht er, MyDoom zu deinstallieren und vorhandene Firewall- und Antiviren-Software zu deaktivieren. Ausserdem installiert er eine neue, eigene Hintertür. Anschliessend verbreitet er sich selbst und befällt weitere MyDoom-verseuchte Rechner. Deren Anwender merken oft nichts davon – eine ideale Ausgangslage für Spammer und Hacker, welche die betroffenen PCs quasi fernsteuern können.

SPAM

Aktiv gegen Müll

Die EU-Kommission fordert mehr Druck beim Kampf gegen die Spam-Plage. Gesetze allein genügten nicht. Die Kommission strebt eine vermehrte internationale Zusammenarbeit, technische Lösungen und Selbstregulierung der Industrie sowie eine stärkere Sensibilisierung der Anwender an. Ausserdem müssten Behörden mit den nötigen Befugnissen zum Aufspüren und Festsetzen von Spammern ausgestattet werden, sagte der zuständige EU-Kommissar Erkki Liikanen. Er forderte eine weltweite Zusammenarbeit bei der Spam-Bekämpfung. Im Gegensatz zur EU, wo Spam grundsätzlich verboten ist, genügt in den USA für legalen Spam eine bestehende Geschäftsbeziehung und die Möglichkeit, sich aus einer Mailingliste auszutragen.

SPAM

Bill Gates kämpft kreativ

In einer Rede hat Bill Gates versprochen, innerhalb der nächsten zwei Jahre sei das Spam-Problem gelöst. Filtertechnologien hätten sich als unzureichend erwiesen. Gates schlägt vor, Versendern von E-Mails zusätzliche Hindernisse in den Weg zu stellen. Er denkt dabei etwa an ein Puzzle, das Absender und Empfänger lösen müssten, oder an eine elektronische Briefmarke, die den Massenversand enorm verteuere – der Spammer müsse zahlen, wenn der Absender seine Post als Spam identifiziere. Microsoft arbeite hart daran, das Spam-Problem zu lösen, so Gates. Bereits liegen Pläne für eine Änderung des SMTP-Protokolls zum Versand von E-Mails vor. Absender, die nicht im Adressbuch des Empfängers stehen, sollen nach den Vorstellungen Microsofts die Mail zurückerhalten und müssen den Versand bestätigen, bevor die Mail endgültig zugestellt wird.

DIALER

Aus für Lustköder

Ab dem 1. April dürfen Webdialer keine 0900er-Nummern mehr anwählen. Das Bundesamt für Kommunikation (Bakom) will damit den bisherigen Missbrauch stoppen. Allein im letzten Jahr seien 2073 Beschwerden betreffend 0900er-Nummern eingereicht worden. Insgesamt musste das Bundesamt 117 Zuteilungen für Nummern widerrufen. Viele Anbieter würden trotz strikter Nutzungsbedingungen die Preise für ihre Dienste nicht klar deklarieren. Bei Download und Installation von PC-Dialern fehle zudem die Transparenz. Auch die Durchführung von Kontrollen sei schwierig. Das Verbot ist für die Anwender allerdings kein Grund zum Aufatmen. Es bedeutet lediglich, dass Opfer von Webdialern nicht mehr zahlen müssen. Allerdings liegt die Beweislast immer noch bei ihnen; sie müssen belegen, dass sie die fragliche Nummer nicht von Hand gewählt haben. Ausserdem können Dialer-Anbieter auf ausländische Nummern ausweichen. Das Bakom hat alle Informationen zum Thema auf der Seite www.bakom.ch/0900 zusammengestellt. *(bha)*

KURZINFOS

«FEUERFUCHS»

Die Mozilla Foundation hat den Webbrowser Firebird (www.pctipp.ch, WEBCODE 25897) und das Mailprogramm Thunderbird (www.mozilla.org/products/thunderbird) auf die Versionen 0.8 bzw. 0.5 aktualisiert. Firebird wird mit dem Upgrade gleichzeitig auch noch in Firefox umgetauft.

MUSIK-DOWNLOAD

Der Europastart der beiden Musik-Download-Plattformen iTunes und Napster verschiebt sich auf die zweite Jahreshälfte. Schuld sind Querelen um Lizenzverträge, unterschiedliche Musikveröffentlichungsdaten und inkompatible Abrechnungssysteme.

SCHLECHT

Die Stiftung «Zugang für alle» hat gemeinsam mit der Namics AG einen Test zur Behindertentauglichkeit von Schweizer Webseiten durchgeführt. Berücksichtigt wurden Homepages von Behörden sowie Diensten wie Internetshops und Online-Banken. Das Ergebnis ist ernüchternd: Nur gerade 8 der 68 getesteten Internetpräsenzen werden als besonders gut für Behinderte geeignet eingestuft.

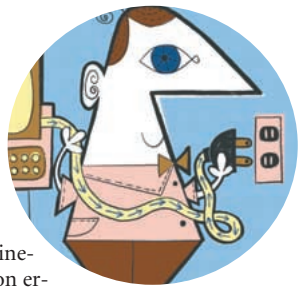
CABLECOM

Zu extremer Spam-Schutz

Zahlreiche Hispeed-Nutzer haben Mails verloren oder erhalten sie mit einer grossen zeitlichen Verzögerung. Grund sind neue Spam-Schutzmassnahmen der Cablecom, die offensichtlich weit übers Ziel hinaus schiessen. Damit eine Mail zugestellt wird, müssen neu gewisse technische Bedingungen beim Absender erfüllt sein (Reverse-DNS: Registrierung beim zuständigen DNS-Server). Das soll gefälschte Absenderadressen verhindern. Das Problem: Zahlreiche Mailserver sind nicht gemäss dem gewünschten technischen Standard eingerichtet. Gleichzeitig sperrt Cablecom ganze Adressbereiche, aus denen häufig so genannte Dictionary Attacks erfolgen: Spammer prüfen anhand von bestimmten Wörtern und Buchstabenkombinationen, ob auf einer Domain eine Mailadresse existiert. Cablecom kündigte kurz nach Bekanntwerden der Probleme Änderungen an.

POWERLINE

EU fördert Internet aus der Steckdose



Um Powerline, den Internetanschluss via Stromnetz, ist es ruhig geworden. Jetzt hat eine EU-Kommission ein neues Förderprojekt ins Leben gerufen, das einen einheitlichen europäischen Powerline-Standard entwickeln soll. Die Kommission erhofft sich davon eine Steigerung des Wettbewerbs im Zugangsnetz. Zudem ermögliche die Technologie, auch strukturschwächere und ländliche Gebiete mit Breitbandinternet zu erschliessen.

ZIP-STANDARD

Einigung

Die beiden Software-Firmen PKWare und WinZip kochten bei den Verschlüsselungsfunktionen ihrer Zip-Programme jeweils ein eigenes Süppchen. Verschlüsselte Archive konnten nicht mehr mit beiden Programmen geöffnet werden. Der Streit hat aber nun glücklicherweise ein Ende. Die neusten Versionen von WinZip und PKZip unterstützen laut Hersteller auch die verschlüsselten Archive der Konkurrenz.

KAZAA

Ärger beim Hauptsitz

Die australische Musikindustrie will Sharman Networks, dem Betreiber der Tauschbörse Kazaa mit Hauptsitz in Sidney, an den Kragen. Die Industrie erwirkte einen Gerichtsbeschluss gegen den angeblich «grössten Urheberrechtsverbrecher der Welt». Polizei und Behörden durchsuchten die Büros von Sharman Networks und dessen Werbepartner Brilliant Digital sowie Privatwohnungen der Mitarbeiter. In den USA hat das Unternehmen seinerseits Klage gegen die Musikindustrie wegen angeblicher Wettbewerbsverletzungen eingereicht.

ILLUSTRATIONEN PJ LOUGHRAN, JANET WOOLEY, MELINDA BECK, JOHN CUENO

ADSL

Alt werden beim Warten auf Tempo

Die ursprünglich auf Mitte Februar angekündigte Bandbreiten-Verdoppelung verzögert sich: Die langsamsten 300-Kbit/s-Anschlüsse werden erst zuletzt, ab dem 1. März, auf 600 Kbit/s umgestellt. Unter Umständen müssen einzelne ADSL-Anwender sogar bis Ende April warten, bis sie vom höheren Tempo auf ihrer Leitung profitieren können. Am schnellsten werden laut der Fachzeitschrift Netzwoche die alten 600-Kbit/s-Anschlüsse umgestellt, dann wird das neue 2400/200-Angebot für Vielsauger eingeführt. Anwender müssen nichts unternehmen, um in den Genuss der neuen Tempi zu kommen. Die Umstellung erfolgt auf Seiten der Swisscom.

GOOGLE

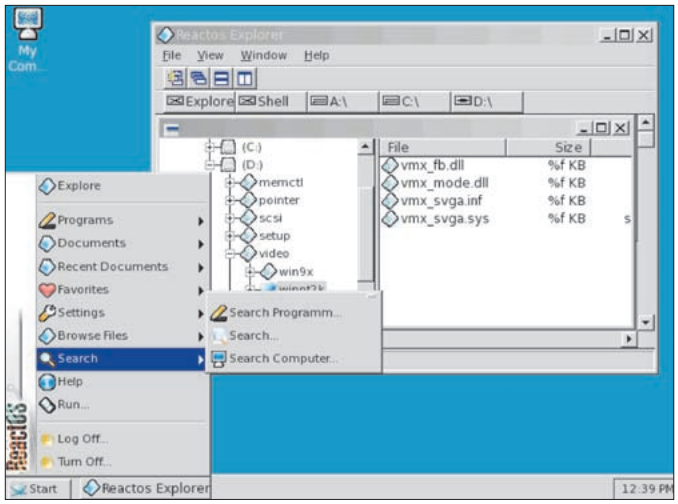
Jobs in Zürich

Google eröffnet in Zürich ein neues Forschungszentrum und sucht Software- sowie Java-Spezialisten (www.google.ch/jobs). Mit ein Grund für die neue Niederlassung der Suchmaschine Nummer eins sind die restriktiven Visa-Bestimmungen der USA. Google begründet die Eröffnung mit dem grossen Potenzial an talentierten Computerwissenschaftlern in Europa, das man sich sichern wolle.

WINDOWS-KLON

ReactOS nimmt Gestalt an

Das neue Betriebssystem ReactOS (www.reactos.com) wird frei entwickelt und hat mit der neuen Version 0.2 einen ersten Meilenstein erreicht. Es bootet eine dem Windows-Explorer ähnliche Oberfläche, den ReactOS Explorer. ReactOS soll vollständig mit Windows NT 4 kompatibel sein; die Entwickler planen zudem für künftige Versionen, auch Windows XP zu unterstützen. Ihr Fernziel: Unter dem komplett neu geschriebenen gratis erhältlichen Windows-Klon sollen alle Windows-Treiber und Windows-Programme laufen. *(bha)*



ReactOS: Der Windows-Klon macht Fortschritte

WINDOWS

Der Herr des Affengriffs ist pensioniert

Jeder Windows-Anwender lernt früher oder später den Affengriff, nämlich die Tasten *Ctrl+Alt+Del* zu drücken. Kaum jemand kennt aber den Erfinder der Finger-Turnübung, mit der unter Windows ein Neustart möglich ist oder der Taskmanager zum Abschiessen hängender Programme geöffnet wird. David Bradley hatte den Warmstart für den ersten IBM-PC innert fünf Minuten programmiert. Auf die Tastenkombination kam er, weil sie sich leicht merken lässt und schwer genug zu drücken ist, um nicht etwa versehentlich den PC neu zu starten. Der Retter von Millionen entnervter PC-Benutzer ist mit 55 Jahren in den Ruhestand getreten. «Ich habs erfunden», scherzte er einmal während einer Veranstaltung, an der auch Microsoft-Chef Bill Gates zugegen war, «aber erst Bill hats berühmt gemacht.» Wohl oder übel.

MAC OS X

Windows ohne Windows

Das neue Projekt Darwine (http://darwine.sourceforge.net) will Windows in Mac OS X integrieren – ganz ohne Windows. Die Entwickler arbeiten auf der Basis von Wine, das auf Linux/Unix-Systemen sozusagen eine «Vermittlungsstelle» zwischen Windows-Anwendungen und dem fremden Betriebssystem bildet. Word & Co. «glauben», sie hätten es mit einem echten Windows-System zu tun. Noch steckt die Entwicklung von Darwine in einem frühen Stadium. Die Installation der bereits herunterladbaren Dateien ist nur versierten Anwendern zu empfehlen. Zudem könnte die Software auf der PowerPC-Plattform noch gar nicht funktionieren.

LINUX

Neues Knoppix mit Kernel 2.6

Knoppix, das beliebte direkt ab CD lauffähige Linux-System, ist in der Version 3.4 erschienen. Das Betriebssystem basiert auf dem Kernel 2.6, der eigentlichen Linux-Basis, der alle Komponenten des PCs steuert. Sie können eine ISO-Datei zum Brennen auf CD hier herunterladen: www.knopper.net/knoppix.

PATENTSTREIT UM IE

Keine Änderungen

Microsoft hat Änderungen am Internet Explorer auf Eis gelegt und will den Ausgang des Berufungsverfahrens gegen die Firma Eolas abwarten. Letzten August hatte ein Gericht Microsoft wegen Patentrechtsverletzung zur Zahlung von einer halben Milliarde US-Dollar an die Firma Eolas Technologies und die Universität von Kalifornien verurteilt. Der Internet Explorer soll eine urheberrechtlich geschützte Technologie verwenden, um externe Anwendungen wie beispielsweise den Media Player aufzurufen. Ursprünglich wollte Microsoft deswegen mit dem kommenden Service Pack 2 für Windows XP einige Modifikationen am Browser vornehmen.

KURZINFOS

AMD-WINDOWS

Microsoft arbeitet an einer 64-Bit-Variante von Windows für die 64-Bit-Prozessoren von AMD. Eine Preview-Version gibts unter www.microsoft.com/windowsxp/64bit/downloads/upgrade.asp.

LINUX-DESKTOP

Die Desktop-Umgebung KDE (www.kde.org) soll in der Version 3.2 deutlich schneller sein. Es bietet neu unter anderem den Musik-Player JuK, den Multi-Instant-Messenger Kopete und die Passwortverwaltung KWallet.