Das Viren-ABC

Nur wer im Cyberspace seinen Gegner kennt, fällt ihm nicht so schnell zum Opfer.

■ von Gaby Salvisberg

Computerschädlinge aller Art (Viren, Würmer, Trojaner etc.) verwenden eine Vielzahl perfider Tricks, um sich zu verbreiten und Schäden zu verursachen. Virenscanner alleine verhindern die drohende Infektion nicht immer. Erweitern Sie Ihr Wissen über die virtuellen Schädlinge, so sind Sie gegen Attacken besser gerüstet.

■ Im Abschnitt «Wurm, Virus & Co.», rechts, erfahren Sie, wodurch sich die verschiedenen Schädlingskategorien unterscheiden und warum es manchmal nicht so einfach ist, ein konkretes Stück böse Software eindeutig einer dieser Kategorien zuzuordnen.

■ In «Schäden» ab Seite 51 zeigen wir, warum Sie einen Schädlingsbefall des PCs keinesfalls auf die leichte Schulter nehmen dürfen, auch wenn der PC anscheinend perfekt funktioniert.

■ Wie sich Schädlinge in Ihre Festplatte einzuschleusen versuchen, verraten wir Ihnen in «Verbreitung», Seite 52.

Wurm, Virus & Co.

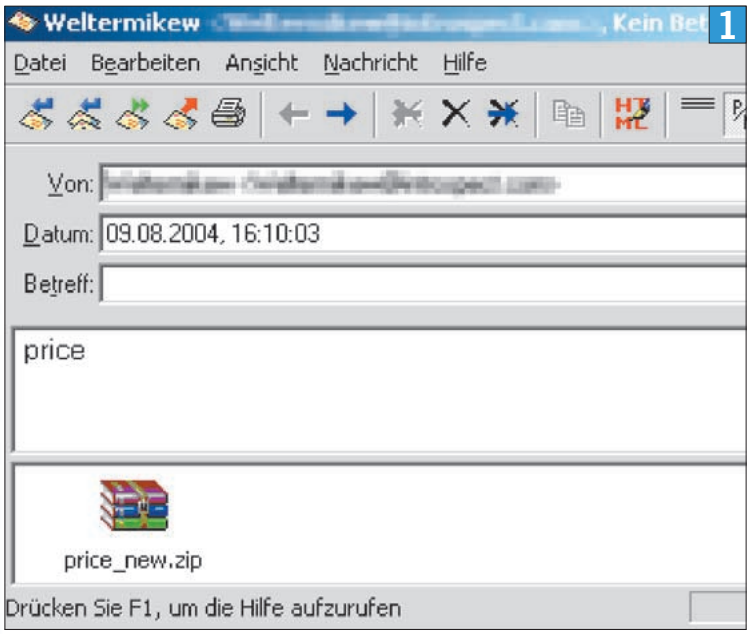
Wann ist ein Schädling als Wurm zu bezeichnen, wann als Virus? Zwar gibt es verschiedene Mischformen von Schädlingen; so kann ein Virus gleichzeitig wurmähnliche Züge aufweisen, während ein Wurm sich nebenbei als «Backdoor» betätigen kann. Es gibt aber durchaus einige grundsätzliche Unterschiede.

Virus: Was ein echter Computervirus sein will, steckt auf dem PC seines Opfers *bestehende* Dateien an. Das heisst, er baut sich selbst bzw. seinen eigenen Programmcode in eine oder mehrere Dateien ein, die er bereits auf dem PC findet. Einige Viren lassen den ursprünglichen Programmcode einer infizierten Datei mehr oder weniger unangetastet. So tut die Datei auf den ersten Blick vielleicht immer noch das Erwartete, wenn sie gestartet wird. Allerdings lädt sie nun zusätzlich und oft unerkannt den neu hinzugefügten Virencode.

Als Träger kann jede Art von ausführbarer Datei herhalten, je nachdem, welche Fähigkeiten der Virenautor seiner «Schöpfung» einprogrammiert hat. Manche Viren spezialisieren sich aufs Infizieren von Programmdateien mit der Endung EXE, andere stürzen sich lieber auf Word-Dokumente mit der Endung DOC. Sind Sie über Letzteres erstaunt? Da alle Office-Dokumente auch → Makros in der Programmiersprache → VBA enthalten können, besteht die Möglichkeit, dass sich darin ein Makrovirus mit seinem Code einnistet.
Tipp: Sollte Ihr Virenscanner in einer Datei einen Virus finden, ist es sicherer, diese von einem sauberen → Backup vollständig auszutauschen, statt den Virenscanner die Datei nur «säubern» zu lassen. Eine gesäuberte Datei entspricht nicht mehr hundertprozentig dem Original und kann unvorhergesehene Störungen verursachen. Bei Makroviren in Office-Dokumenten ist das Säubern manchmal unumgänglich, hier ist der Vorgang allerdings meistens von Erfolg gekrönt.

Bootbereichvirus: Eine spezielle Virenart nistet sich im Bootbereich von Datenträgern ein. Dieser Bereich von Festplatten oder Disketten nimmt

ILLUSTRATION TOM HÜBSCHER, TNT-GRAPHICS



Der berüchtigte Bagle-Wurm verbreitet sich per Anhang in E-Mails

Informationen auf, wie das Betriebssystem aufgestartet werden soll. Wird ein PC ab einer infizierten Diskette gestartet, kann sich der Virus auf die Festplatte übertragen und von dort wiederum auf noch saubere Disketten. Heute werden Dateien jedoch viel häufiger per E-Mail verschickt als per Diskette. Deshalb sind Bootbereichviren vergleichsweise selten geworden.
Tipp: Disketten lassen sich einfach vor Virenbefall schützen, indem Sie den Schreibschutz-Schieber umschalten.

Wurm: Würmer infizieren keine bestehenden Dateien, sondern legen auf dem infizierten PC *neue* Dateien ab oder ersetzen bestehende Files durch Kopien von sich selbst. Das bedeutet: Wenn ein Virenscanner in einer Datei einen Wurm findet, dann gehört die ganze Datei zum Wurm, es ist also nicht möglich, sie zu desinfizieren.

Würmer verbreiten sich nicht nur mit per E-Mail verschickten Dateien, Screen 1, sondern attackieren bisweilen auch Sicherheitslecks in der Internetverbindung bestimmter Betriebssysteme. Im Januar 2003 machte der Slammer-Wurm von sich reden, der es auf Systeme mit einem installierten Microsoft-SQL-Server (eine bestimmte Art von Datenbank) abgesehen hatte. Er legte keine Dateien ab, sondern installierte sich in den Arbeitsspeicher der betroffenen Maschinen. Die enorme Anzahl der so infizierten Server sorgte für derart viel überflüssigen Datenverkehr, dass viele Webseiten nicht mehr erreichbar waren.

Trojaner: Korrekt müsste es «Trojanisches Pferd» heissen, in Anlehnung an das Holzpferd aus der griechischen Mythologie. Solche Schadensprogramme versuchen, sich als etwas anderes auszugeben – etwa als nettes Spiel oder nützliches Programm. Im Gegensatz zu Viren und Würmern verbreiten sich Trojaner nicht aus eigener Kraft. Stattdessen werden sie auf Webseiten oder in Tauschbörsen als etwas anderes angepriesen oder per Spam verschickt.
Tipp: Setzen Sie nur auf vertrauenswürdige Quellen, wenn Sie eine Software herunterladen.

Backdoor: So werden Schädlinge genannt, die in der Internetverbindung eine Hintertüre einrichten. Je nach Art dieser Hintertüre kann ein Angreifer Daten auf dem PC ausspionieren oder zusätzliche unerwünschte Programme einschmuggeln.

Schäden

Die Schäden, die das Ungeziefer anrichtet, sind beträchtlich, meist sind die Symptome aber nicht auf den ersten Blick erkennbar. Kein Wunder: Ein Virus oder Wurm, der auf sich aufmerksam macht, läuft Gefahr, entdeckt und gelöscht zu werden. Also werden sich die meisten Schädlinge davor hüten, ihre Opfer durch Anzeigen von Sprüchen oder grafischen Effekten mit der Nase darauf zu stossen, dass etwas faul ist. Es gab auch hier Ausnahmen, wie der Hybris-Virus bewies. Dieser konnte aus einer → Usenet-Newsgroup zusätzliche Module nachladen, die zum Beispiel bewirkten, dass der infizierte PC plötzlich eine schwarzweisse Spirale anzeigte, die sich nicht wegklicken liess.

Mailflut: Wenn sich Viren oder Würmer massenhaft per E-Mail verschicken, verstopfen sie Postfächer und belasten Internetverbindungen und Server. Dies war eine besondere Spezialität des Swen-Wurms: Er überflutete von infizierten PCs aus die Adressen seiner Opfer mit Attachments von 150 Kilobyte Grösse. ▶

FACHCHINESISCH

Makro

Ein Makro ist ein Werkzeug zur Automatisierung wiederkehrender Arbeitsschritte innerhalb von Anwendungsprogrammen. Makros können meist einfach mit einem «Recorder» aufgezeichnet und abgespielt werden, lassen sich aber oft auch mit einer integrierten Programmiersprache beschreiben.

VBA

VisualBasic for Applications (VBA) ist die Programmiersprache, die in Microsoft-Office-Programmen (Word, Excel etc.) für Makros verwendet wird.

Backup

Regelmässiges Sichern von Daten auf externe Datenträger wie z. B. CD-ROM, DVD oder Bandlaufwerke. Je nach verwendeter Hard- und Software lässt sich ein Backup auch automatisieren.

Usenet-Newsgroups

Ein Bereich des Internets, in dem die Internetteilnehmer über die verschiedensten Themen miteinander diskutieren und Tipps austauschen. Diese digitalen «schwarzen Bretter» können mit einem Newsreader (z. B. Mozilla Thunderbird, NewsPro oder Forté Agent) gelesen werden.

Datenverlust: Bei so manchem Schädlingsbefall geraten die persönlichen Dateien des Benutzers in Gefahr. Einige Varianten des Loveletter-Wurms löschten zum Beispiel auf der Festplatte gespeicherte Musikstücke im MP3-Format oder JPEG-Bilder.

Um Dateien, die für den *Betrieb* des PCs wichtig sind, machen die meisten Viren und Würmer jedoch einen Bogen. Nicht ohne Grund: Von einem PC aus, der nicht mehr läuft, kann sich ein Schädling nicht mehr weiterverbreiten. Natürlich bleibt auch diese Regel nicht ohne Ausnahme. Der CIH-Virus, der vor rund sechs Jahren erstmals sein Unwesen trieb, überschrieb unter gewissen Umständen nicht nur die Festplatte des infizierten PCs, sondern versuchte auch, dessen Flash-BIOS mit Mülldaten zu überschreiben. Weil er damit aber meist bis zum 26. Tag des Monats wartete, hatte er zuvor genügend Zeit, sich zu vermehren.

Datenveränderung: Fast noch bedenklicher als das Löschen von Dateien wäre deren Manipulation. Stellen Sie sich einen Wurm vor, der in zufällig ausgewählten Zellen von Excel-Tabellen oder Datenbanken einfach die Werte ändert. Es wäre fast unmöglich herauszufinden, welche Zellen vom Wurm verändert wurden. Dieses Verhalten wurde in freier Wildbahn zwar bisher kaum beobachtet, ist aber denkbar. Immerhin gabs schon Word-Makroviren, die Texte in Dokumenten veränderten.

Tipp: Besonders Daten, die Sie mit grossem Aufwand erstellt haben, sollten Ihnen ein tägliches Backup wert sein. Bewahren Sie davon mehrere ältere Varianten auf.

Spionage und Missbrauch des PCs: Lange Zeit war das Einpflanzen von Backdoors (siehe S. 51) das alleinige «Hobby» von Trojanern. Inzwischen öffnen aber auch viele E-Mail-Würmer solche Hintertüren. Das kann peinliche Folgen haben: Wer diese Türen zu benutzen weiss, ist fähig, einen infizierten PC via Internet fernzusteuern und Dinge tun zu lassen, von denen der Besitzer nicht das Geringste mitbekommt. PCs, die auf diese Weise kompromittiert wurden, sind zum Beispiel bei Spammern sehr beliebt. Diese verschicken die unerwünschten Werbemails nicht mehr direkt vom eigenen PC an die genervten Empfänger, sondern nutzen die infizierten Computer als Verteilstationen. So bekommt nicht der Spammer Ärger mit seinem Provider, sondern der Benutzer, dessen PC in eine Spam-Schleuder verwandelt wurde.

Computer mit solchen Backdoors werden von → Crackern und Virenschreibern bisweilen auch für ganz andere Aktivitäten missbraucht. So lassen sich ganze Armeen solcher PCs zu einer Art Netz zusammenschliessen, das Angriffe auf bestimmte Webseiten ausführt. Häufige Opfer solcher so genannten «Distributed Denial-of-Service Attacks» sind zum Beispiel die Server von Regierungen, grosser Firmen oder Antispam-Organisationen. Deren Webseiten sind dann zum Teil über Stunden hinweg nicht erreichbar, manchmal brechen die Server sogar unter der Last der Angriffe zusammen.

Das Ausspionieren von Passwörtern oder Kreditkartennummern kommt natürlich auch immer noch vor.

Der Antiviren-Software-Hersteller Trend Micro zeigt auf seiner Homepage, welche Viren wo verbreitet sind

Verbreitung

Genauso vielfältig wie die möglichen Schäden durch Viren oder Würmer sind auch deren Verbreitungsmethoden. Einige Würmer setzen auf mehrere Standbeine (z. B. Mail und Tauschbörsen), um in möglichst kurzer Zeit eine grösstmögliche Verbreitung zu erlangen, Screen 2. Hier die wichtigsten und häufigsten Verbreitungswege:

Massenmails: Die simpelste und häufigste Methode der Verbreitung ist natürlich E-Mail. Dabei verschickt ein infizierter PC den Wurm oder Virus vollautomatisch an alle Adressen, die er auf der Festplatte findet. Das können Adressen in den Outlook-Kontakten sein oder solche von Webseiten, die der Benutzer besucht. Weil Würmer meist nicht ein installiertes Mailprogramm wie Outlook oder Outlook Express benutzen, sondern selbst eine Mailversandfunktion mitbringen, findet man die so verschickten Mails nicht im Postausgang oder in den gesendeten Mails.

Seit Anfang Jahr fällt auf, dass Virenschreiber ihre unerwünschten Kreationen zu Anfang mit Spammer-Methoden – also unter Verwendung von ganz normalen E-Mail-Adresslisten – in Umlauf bringen, um eine möglichst hohe Infektionsrate zu erzielen.

Tipp: Mailwürmer verbreiten sich schnell. Auch das neuste Update Ihres Virenscanners kann unter Umständen nicht neu genug sein. Eine Mail kann also einen Virus enthalten, auch wenn der Virenscanner nicht Alarm schlägt.

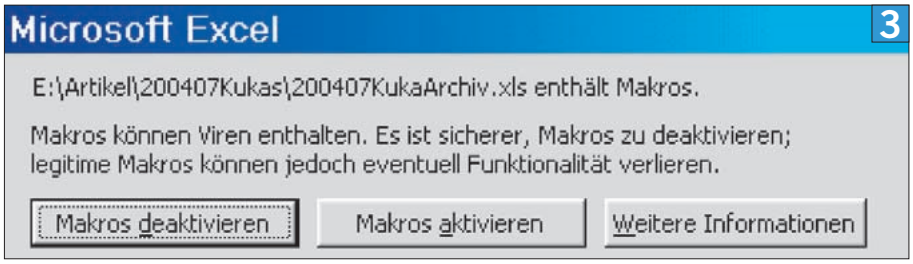
Infektion von Dateien: Handelt es sich beim Schädling um einen Virus, pflanzt er seinen Programmcode in bestehende Dateien ein (siehe S. 50). Nun braucht er nur noch zu warten, bis der Benutzer eine der infizierten Dateien weitergibt. Der Empfänger führt die Datei aus und schon ist sein PC infiziert – sofern nicht der Virenscanner vorher einschreitet. Der zerstörerische CIH-Virus wurde im Jahr 1999 unter anderem von infizierten Exemplaren des beliebten Moorhuhn-Spiels verbreitet. Dieses haben sich die Benutzer damals gegenseitig massenhaft zugemailt.

Dasselbe gilt auch für unzählige Varianten der Office-Makroviren. Weil es heute immer noch sehr beliebt ist, Word- oder Excel-Dateien per Mail zu verschicken, sind Makroviren noch längst nicht ausgestorben. Sobald ein Benutzer zum Bei-

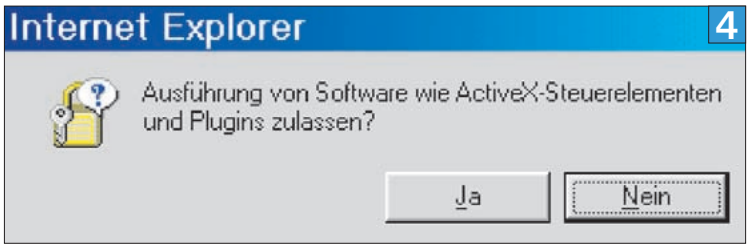
→ FACHCHINESISCH

Cracker

Ein Cracker ist eine Person, die mutwillig übers Internet Daten klaut oder zerstört. Wer hingegen ohne zerstörerische Absicht in ein System eindringt, wird Hacker genannt.



Der Makrodialog von Excel: Woher soll der Benutzer wissen, ob das Makro gut oder böse ist?



Wer kann denn sicher entscheiden, ob JA oder NEIN?

spiel eine infizierte Word-Datei öffnet, überträgt sich der darin enthaltene Makrovirus normalerweise auf die Standardvorlage Normal.dot. Von diesem Zeitpunkt an ist jede neue Word-Datei infiziert. Ein Extremfall war zweifelsohne der Makrovirus Melissa. Dieser verschickte zusätzlich automatisch ein infiziertes Word-File an die ersten 50 Kontakte des Outlook-Adressbuchs.

Tipp: Microsoft Office hat eine Art eingebauten Makroschutz. Für bestmögliche Makrosicherheit stellen Sie diesen in den Office-Programmen im Menü EXTRAS/MAKRO/SICHERHEIT auf «Hoch» bzw. schalten in älteren Versionen unter EXTRAS/OPTIONEN/ALLGEMEIN den «Makrovirus-Schutz» ein.

Freigaben und Tauschbörsen: Einige bekannte Würmer suchen auf dem infizierten PC nach einer installierten Tauschbörsen-Software wie z. B. eMule oder Gnutella. Dann machen sie den Ordner ausfindig, den der Benutzer ins Tauschbörsennetz freigegeben hat, und kopieren sich dorthinein. Jetzt braucht so ein Wurm nur noch darauf zu warten, dass sich jemand freiwillig diese Dateien herunterlädt und installiert. Die Chance, dass dies mehr als einmal passiert, erhöht sich durch Social-Engineering-Tricks erheblich (siehe S. 54). So tragen die Schädlingskopien besonders verlockende Dateinamen, beispielsweise «WinXP_Seriennummern Crack.exe», «Office 2003 Keygenerator.exe» oder für die schlichteren Gemüter «Britney Spears nude.jpg.exe».

Lücken: Sobald eine Sicherheitslücke in Windows oder im Internet Explorer entdeckt oder gar publik wird, besteht die Gefahr, dass Cracker diese ausnutzen. Besonders Netzwerkwürmer wie Blaster oder Sasser haben solche Sicherheitslecks verwendet, um sich völlig ohne Zutun des Anwenders von einem verwundbaren PC zum nächsten zu verbreiten.

Tipp: Die Updates zum Stopfen neu entdeckter Löcher lassen manchmal auf sich warten. Newsletter von Software-Herstellern oder von www.pctipp.ch/newsletter informieren Sie unter anderem über neue Lücken – oft sogar mit Tipps, wie Sie die Sicherheitslücke selbst entschärfen können.

FACHCHINESISCH

ActiveX

Eine von Microsoft entwickelte Programmiersprache, die das Ausführen von Programmen direkt auf einer Webseite erlaubt. Sie funktioniert aber nur mit dem Internet Explorer.

Browser-Hijacker

Ein meist unerwünschtes Programm, das im Webbrowser Einstellungen verändert, wie zum Beispiel die Adressen der Start- und Suchseiten.

IP-Adresse

Jeder PC, jeder Computer, der mit dem Internet verbunden ist, braucht während der Online-Sitzung (also während er online ist) eine eindeutige IP-Adresse, um mit anderen Computern – wie z. B. einem Web- oder Mailserver – zu kommunizieren. Diese IP-Adresse («Internet Protocol»-Adresse) ist eine solche Kennung, die meist bei der Einwahl vom Internetprovider (ISP) vergeben wird.

«Features»: Abgesehen von den unabsichtlich vorhandenen Löchern gibts auch absichtlich in Software einprogrammierte Fähigkeiten, die durch Schädlinge missbraucht werden. Allen voran wie erwähnt die Makrofähigkeit vieler namhafter Programme. Microsoft musste in seine Office-Programme nachträglich Sicherheitsmechanismen einbauen, mit denen die Anwender gewarnt werden, wenn sich in Dokumenten Makros befinden. Makros können aber auch gut und nützlich sein. Ganz auf sie zu verzichten hiesse, Office nicht mehr voll zu nutzen. Trotzdem hat Microsoft noch keinen für den Benutzer zumutbaren Weg gefunden, nützliche von unerwünschten Makros zuverlässig zu unterscheiden, Screen 3.

Das zweite Beispiel für häufig missbrauchte Programmfähigkeiten ist der Internet Explorer und seine Vorliebe für → ActiveX-Controls. So lange diese auf der Windows-Update-Seite die neusten Patches holen oder einem Online-Virenscanner beim Virensuchen helfen, sind sie ganz nützlich. Ganz und gar unerwünscht ist jede ActiveX-Fähigkeit, wenn sie einer Spyware oder einem → Browser-Hijacker zur erfolgreichen Installation verhilft. Hand aufs Herz: Wie viele Benutzer sind vernünftig genug, auf NEIN statt auf JA zu klicken, wenn ihr Browser sie um Script-Ausführ-Erlaubnis bittet, Screen 4? Dummerweise verlangt der Internet Explorer sogar zum Ausführen von Plug-Ins (z. B. Macromedia Flash) ein eingeschaltetes ActiveX.

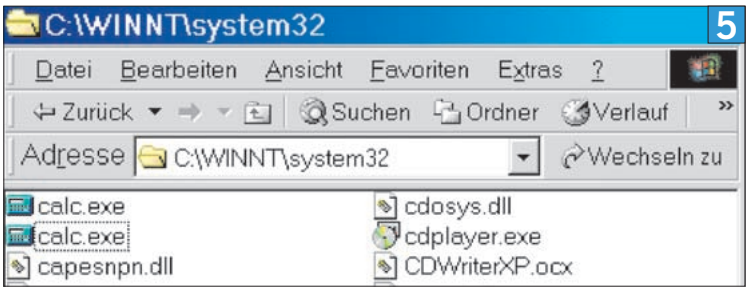
Tipp: Fürs tägliche Surfen empfehlen wir den Umstieg auf einen anderen Browser, wie zum Beispiel Mozilla, Firefox oder Opera, zu finden unter www.pctipp.ch/downloads.

Virenscanner blockieren: Je mehr Zeit ein Virus oder Wurm für seine Verbreitung hat, desto mehr PCs kann er anstecken. Deshalb versuchen viele Schädlinge, ihrer Entdeckung und Beseitigung zu entgehen. Hierfür arbeiten sie mit unterschiedlichen Tricks: Würmer können Webadressen (z. B. www.mcafee.com der Antivirenfirma McAfee) auf eine andere → IP-Adresse umleiten; etwa auf 127.0.0.1, die immer auf den eigenen Computer zeigt. Die Folge ist, dass der Browser unter www.mcafee.com keine Webseite mehr findet. Damit verhindern Schädlinge, dass der Benutzer sich von kompetenter Stelle Online-Hilfe holt.

Eine beliebte Schädlingstaktik ist die Überwachung der im Hintergrund laufenden Prozesse. Entdeckt ein Wurm, dass eine EXE-Datei gestartet wurde, die zu einer Antiviren-Software oder einem Windows-Hilfsprogramm gehört, schiesst der Wurm diesen Prozess sofort ab. Schliessen sich also der Windows-Taskmanager oder Ihr Virenscanner nach dem Start sofort wieder, könnte dafür ein Schädling verantwortlich sein. ▶

Social Engineering

So nennt sich die Kunst des Übertölpelns von Mitmenschen, damit diese sich zu Dingen hinreissen lassen, die sie sonst vielleicht nicht tun würden. Wir zeigen hier einige typische Social-Engineering-Tricks, die Virenschreiber verwenden, um die Benutzer unter anderem zum Öffnen von Virenfiles zu bewegen.



Zweimal denselben Namen darf man nicht verwenden. Doch welches ist die echte Datei?

Gefälschte Absenderadressen: Würmer verschicken sich von infizierten PCs aus automatisch. Dabei wird als Absender praktisch nie die richtige Adresse des PC-Inhabers verwendet. Stattdessen steht entweder eine andere auf dem PC gefundene Adresse drin oder eine, die sich der Schädling selbst ausdenkt oder aus gefundenen Domain-Namen zusammensetzt. Das ist besonders perfid, wenn die Mail dadurch den Anschein bekommt, sie käme von einer seriösen Firma. Wer würde einer offiziell aussehenden Mail von «info@microsoft.com», «support@ihrprovider.ch» oder gar «service@pctipp.ch» nicht trauen?

Antwort auf Ihre Mail: Genau wie es viele Spammer tun, gibts auch Mailwürmer, die den Betreff der Mails mit «RE:» beginnen. Dies soll den Anschein erwecken, die Mitteilung sei eine Antwort auf eine Mail, die man selbst verschickt hat. Es gab sogar schon Würmer, die tatsächlich alle neu eintreffenden Mails automatisch beantworteten; natürlich mit einem möglichst allgemein klingenden Text und der unvermeidlichen schädlichen Beilage.

Angeblich virengeprüft: Einige Virenscanner fügen bei ausgehenden Mails eine Signatur wie diese hinzu: «Diese Mail wurde durch 'Produkt namens XY' auf Viren geprüft.» Schon längst gibt es Mailwürmer, die ausgerechnet solche Mailsignaturen bekannter Antivirenhersteller abkupfern. Ein Text wie «Diese Mail ist virenfrei» innerhalb einer Mail ist deshalb heute kein Grund mehr, einer Mail zu trauen; eher im Gegenteil.

Doppelte Dateiendungen: Windows blendet standardmässig bekannte Dateiendungen aus, deshalb wird zum Beispiel eine Datei namens «UnserBüsi.jpg.exe» eben nur als «UnserBüsi.jpg» angezeigt. Die echte Endung (EXE), die darauf hindeutet, dass die Datei ein Programm ist und somit gefährlich, wird nicht angezeigt und der Benutzer hält die Datei für ein harmloses JPG-Bild. **Tipp:** Bringen Sie Windows dazu, Ihnen möglichst alle Dateiendungen anzuzeigen. Wie das geht, lesen Sie in «Tipps gegen den Virenkater», PCtipp 4/2004, S. 28, oder unter www.pctipp.ch mit WEB-CODE **pdf040428**. Ist dies erledigt, haben Sie es etwas einfacher: Wenn eine Datei unter Windows eine doppelte Endung aufweist, ist sie verdächtig.

Systemdateiähnliche Namen: Bei der Installation auf einem PC verwenden viele Schädlinge Dateinamen, die jenen von Windows-Programmdateien sehr ähnlich sehen. Statt eines kleinen

«L» (bzw. «l») wird ein grosses «i» (bzw. «I») verwendet. Je nach Schriftart sind diese beiden Buchstaben kaum mehr auseinander zu halten. In Screen 5 ist nicht auszumachen, welche der beiden Windows-Taschenrechner-Dateien wirklich die Originaldatei (calc.exe) ist.

ZIP-Datei suggeriert Sicherheit: Neuste Würmer legen die schädlichen Dateien oft nicht mehr direkt in die automatisch verschickten Mails, sondern packen diese in eine ZIP-Datei, die manchmal sogar durch ein Kennwort geschützt ist, das der Benutzer zum Öffnen der Datei eingeben soll.

Damit erwischt ein Schädling gleich zwei Fliegen auf einen Schlag: Erstens werden ZIP-Dateien von den meisten Mailservern und Mailprogrammen standardmässig nicht blockiert. Ist die Datei darüber hinaus noch passwortgeschützt, kann ein Virenscanner sie oft gar nicht scannen. Zweitens haben Benutzer tendenziell weniger Angst vor ZIP-Dateien. Besonders wenn dann noch etwas im Text steht wie dies: «Um die Datei vor Viren zu schützen, haben wir sie in ein passwortgeschütztes Zip-File gepackt.» Das ist natürlich Unsinn und soll Sie nur in falscher Sicherheit wiegen.

Tipp: Nicht alle Virenscanner sind fähig, ZIP-Dateien zuverlässig zu prüfen. Anders zum Beispiel jener von Kaspersky. Mit dessen Online-Version prüfen Sie einzelne Dateien, auch wenn diese gezippt sind. Sie finden ihn unter www.kaspersky.com/de/scanforvirus. Bedenken Sie aber, dass auch Kaspersky bei neuen Schädlingen einige Stunden braucht, bis der Scanner diese erkennt.

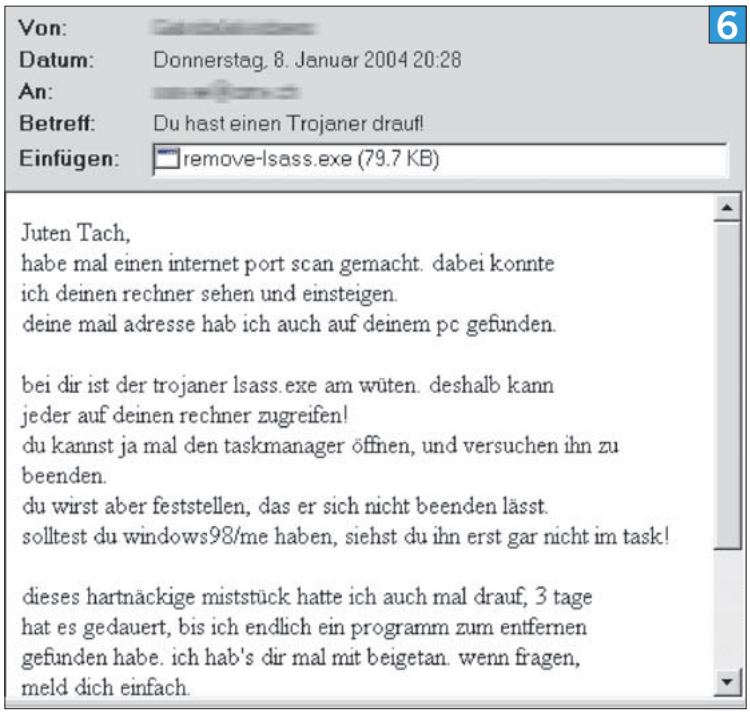
Nachahmen typischer Mails: Haben Sie sich bei einer Mailadresse vertippt, erhalten Sie vom Zielserver oft eine Nachricht, die Mail sei nicht zustellbar. Viele Würmer verschicken selbst Mails mit dem Wortlaut der Unzustellbarkeits-Benachrichtigungen. Wer in der Beilage nachschauen will, welche Mail ihr Ziel verfehlt hat, erlebt eine böse Überraschung: Statt der Kopie einer angeblich verschickten Mail steckt der Wurm drin.

Tipp: In solchen Fällen dürfen Sie Beilagen nur öffnen, wenn es sich wirklich um echte Textdateien handelt. Öffnen Sie solche Dateien auch niemals via Doppelklick. Starten Sie stattdessen unter Start/Programme/Zubehör zuerst den Notepad-Editor und öffnen Sie die Datei darin via Datei/Öffnen. Auf diese Weise wird allenfalls enthaltener Virencode nicht ausgeführt.

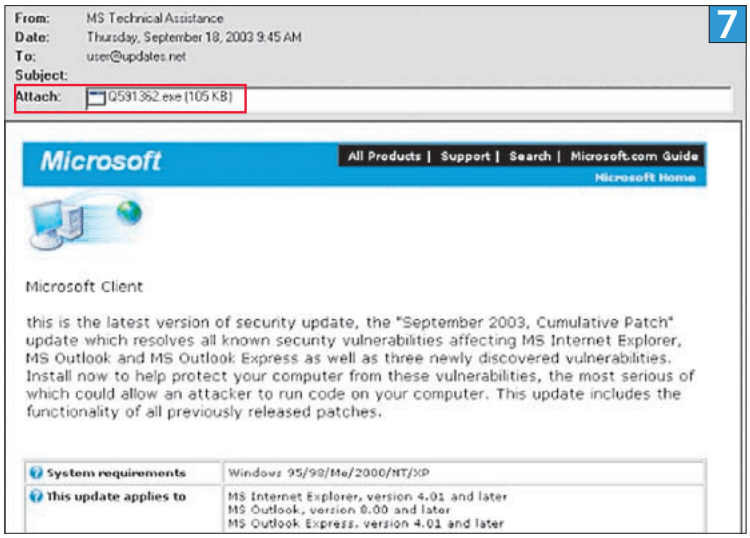
«Patch in der Beilage»: Eine E-Mail wie «Ihr PC hat uns einen Virus geschickt. Beseitigen Sie ihn mit dem beiliegenden Reparaturprogramm», Screen 6, ist ein besonders schönes Stückchen Social Engineering.

Das Gleiche gilt für angebliche Mails von Microsoft, die behaupten, die Beilage sei ein Patch für eine besonders gefährliche Sicherheitslücke. Besonders überzeugend sahen zum Beispiel die Mails des Swen-Wurms aus, Screen 7.

Tipp: Niemals würde Microsoft oder eine andere seriöse Firma solche Patches oder Reparaturprogramme unaufgefordert per E-Mail verschicken. Wenn solche Mails mit ausführbarer Beilage ankommen, ist es fast sicher ein Wurm – egal, wie seriös die Mail klingen oder aussehen mag.



6 **Der Wurm Sober.C tut, als sei er ein Trojaner-Beseitigungs-Werkzeug**



7 **Eine Mail mit täuschend echtem Microsoft-Aussehen, aber mit dem Swen-Wurm als Beilage**

Sex, Angst und Gier: Was Spammer schon längst wissen, nutzen auch Virenschreiber. Sie setzen heute vermehrt auf Mailtexte und Dateinamen, die an Instinkte und Gefühle wie Sex, Angst und Gier appellieren. Die Aussicht auf das Bild eines nackten Pop-Sternchens oder auf die gecrackte Gratisversion einer teuren Software verleitet unzählige Benutzer zum übereilten Klick auf eine verheissungsvolle Datei. Das zieht in E-Mails immer noch genauso gut wie in Tauschbörsenprogrammen.

Der Wurm Sober.C versetzte die Empfänger seiner Mails auch hie und da in Panik: Er verwendete Betreffzeilen wie «Ich zeige Sie an!». Natürlich steckte in der Beilage der Mail nicht das angebliche Beweismittel für die drohende Anzeige, sondern eine Kopie des Wurms.

Verwendete Sprache: Auch wenn immer noch zu viele Mailbenutzer auf Wurmmails hereinfallen, werden einige doch skeptisch, wenn z. B. ein Kollege plötzlich in Englisch schreibt statt wie gewohnt in Deutsch. Deshalb führen viele Mailwürmer mehrere Sprachversionen ihrer Mailtexte mit. Wenn sie sich an Adressen mit Endung .at, .ch oder .de verschicken, steht der deutschsprachige Mailtext drin, bei Adressen auf Endung .com oder .net der englische etc.

Noch mehr Sicherheitstipps

Wie Sie Ihr System in Schuss halten, können Sie in diesen PCtipp-Artikeln nachlesen:

- Service Pack 2 für Windows XP, «Sicherheitskur für XP», PCtipp 9/2004, Seite 6, WEBCODE pdf040906.
- Tipps gegen «Spyware und Hijacker», PCtipp 8/2004, ab Seite 22, WEBCODE pdf040822.
- Kaufberatung Sicherheits-Software, «Sicherer Schutz», PCtipp-Spezial Herbst 2004, S. 59, jetzt am Kiosk. ■