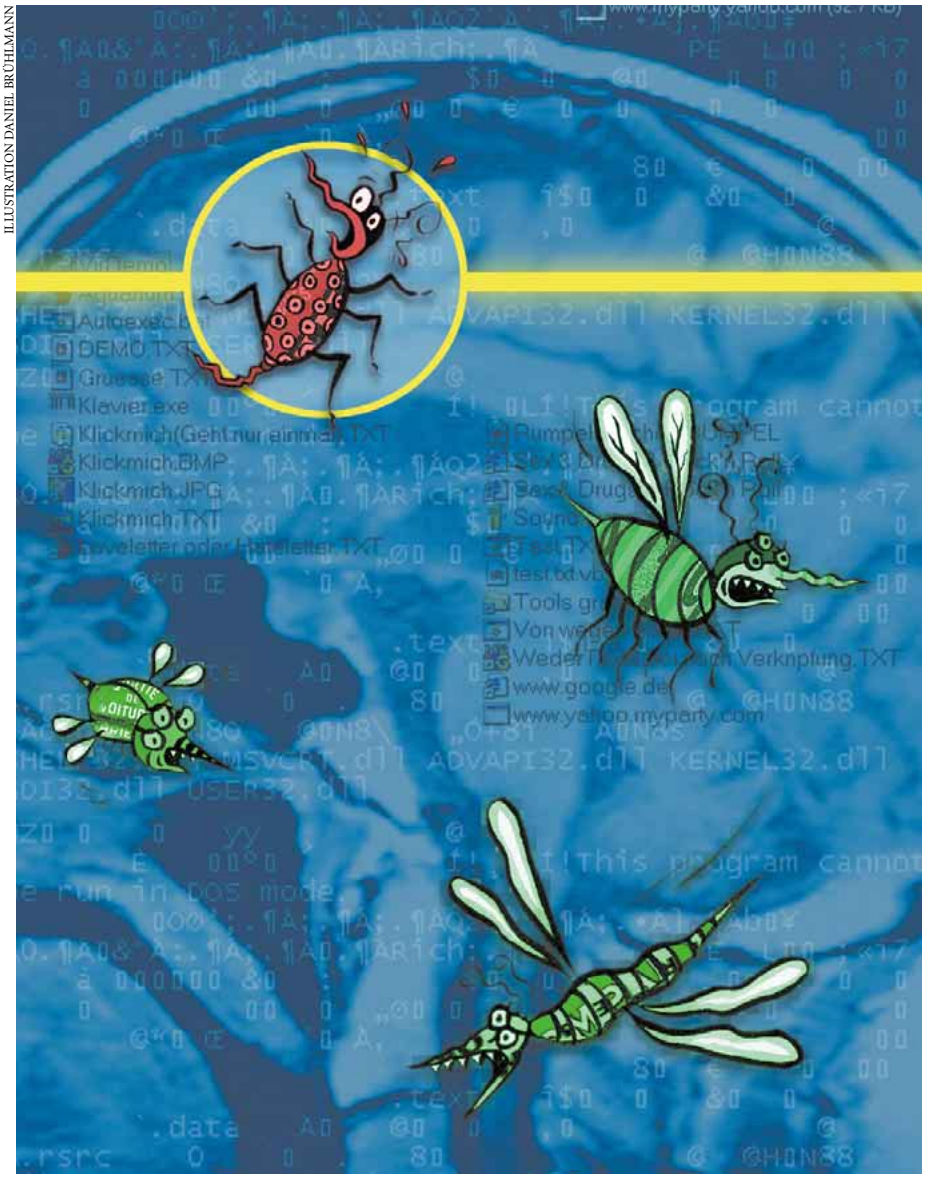
ILLUSTRATION DANIEL BRÜHLMANN



Ihr Hirn als Virenscanner

Virenscanner können brandneue Viren, Würmer und Trojaner übersehen. Mit Hilfe der Dateiendungen unterscheiden auch Sie Gut von Böse.

von Hermann Apfelböck und Christian Löbering

Egal, ob subtiler Virus oder primitiver Kahlschlag-Trojaner: Computer-Schädlinge sind meist so konstruiert, dass der Anwender selbst den entscheidenden Fehler (sprich einen Doppelklick) machen muss, um sie zu aktivieren. Oft werden PCs mit Schädlingen infiziert, weil den Benutzern nicht klar war, dass in der Mailbeilage die Gefahr lauerte. Deshalb geht es in erster Linie darum, ausführbaren → **Code** (Programme, → **Scripts**) aus fremder Quelle konsequent zu vermeiden.

Welche Dateien gefährlichen Code enthalten können oder auf solchen verweisen, ist heute nur noch schwer zu durchschauen. Zu den früher typischen Programmdateien mit den Endungen EXE und COM gesellt sich inzwischen eine ganze Palette weiterer riskanter Dateitypen. Ausserdem nutzen die Programmierer der Schädlinge jeden Kniff, um gefährliche Dateien wie harmlose Text- oder Bilddateien aussehen zu lassen. Auf den folgenden Seiten erhalten Sie einen Überblick über potenziell gefährliche Dateitypen und die typischen Tarnmechanismen.

Tipp: Bei unserer Schwesterzeitschrift PC-Welt können Sie eine kleine Sammlung harmloser Demodateien herunterladen, um die in diesem Artikel beschriebenen Phänomene nachzuvollziehen oder Ihre Einstellungen zu testen, **Screen 1**: **http://www.pcwelt.de/downloads/sonstiges/aktuelle software/26457/**.

Programme mit Endungen EXE und COM: Schädlinge, die als Programmdateien (Endung EXE oder COM) daherkommen, stellen die grösste Gefahr für Ihr System dar. Sobald ein Programm ausgeführt wird und im Arbeitsspeicher sitzt, hat es die volle Kontrolle über ein System. Komplexe Schädlinge basieren in der Regel auf solchem (meist verschlüsseltem) Programmcode. Einfachere Viren oder Würmer verwenden auch Scripts.

Wahrscheinlich werden künftige Schädlingsprogrammierer die Endung COM bevorzugen, weil das psychologisch wirkungsvolle Tarnmöglichkeiten eröffnet: Eine Beilage mit einem Namen wie «www.myparty.yahoo.com» sieht wohl wie ein Web-Link aus, kann aber in Wahrheit Programm- bzw. Virencode enthalten. Diverse EXE-Viren verzichten aber noch heute auf jede Tarnung und vertrauen auf die Wirkung von Dateinamen wie PASSWORD.EXE oder READ-ME.EXE, **Screen 2**.

Tarnung mit PIF und SCR: Die Endungen PIF und SCR werden derzeit am häufigsten zum Tarnen von Schädlingen eingesetzt. Die Dateiendung SCR verspricht eigentlich einen Screensaver (Bildschirmschoner), erlaubt allerdings auch das Ausführen jedes anderen Windows-Programmcodes (etwa EXE). Der Dateityp PIF (Program Information File) wurde ursprünglich für Verknüpfungen zu DOS-Programmen unter Windows verwendet, kann aber ebenfalls Pro-

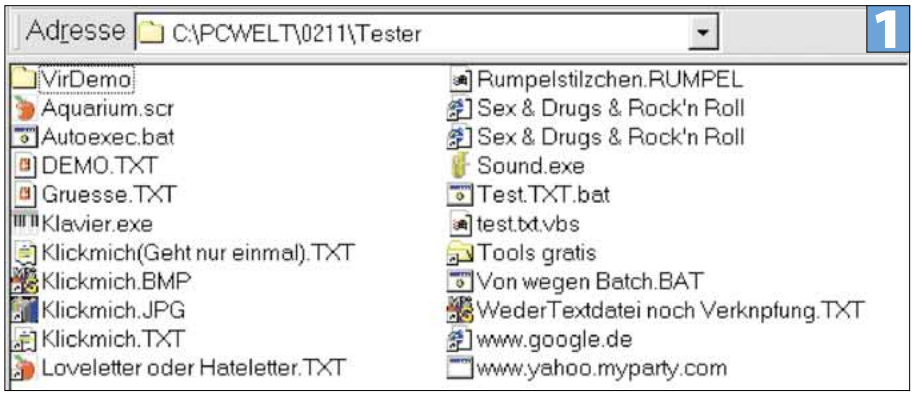
gramme enthalten. Die Endung PIF ist bei Virenprogrammierern besonders beliebt. Kein Wunder, zeigt Windows doch diese Endung grundsätzlich nicht an – anders als SCR und ungetarnte EXE- oder COM-Dateien. Das hat die Virenschreiber zu typischen Mailanhängen wie HAMSTER.DOC.PIF animiert. Der Anwender sieht nur den Namen der vermeintlichen Word-Datei «HAMSTER.DOC», doch was er ausführt, ist ein EXE-Programm.

Scripts mit Endungen VBS, HTM & Co.: Bei Dateien mit den Endungen HTA, HTM, HTML, JS, JSE, VBS, VBE und WSF handelt es sich um Script-Code im einfachen Textformat. Abgesehen von VBE und JSE («e» für «encoded», verschlüsselt) ist deren Inhalt zum Beispiel mit dem Notepad-Editor lesbar (siehe Box «Aufgedeckt», S. 27). Die Fähigkeiten solcher Scripts entsprechen etwa jenen von → **VBA-Makros**. Dennoch sind sie weitaus gefährlicher, weil sie der zuständige → **Script-Interpreter** ohne Vorwarnung ausführt. Wesentliche Unterschiede im Gefahrenpotenzial der einzelnen Endungen bestehen nicht, sie binden in der Regel Scripts ein, um an ihr Ziel zu gelangen.

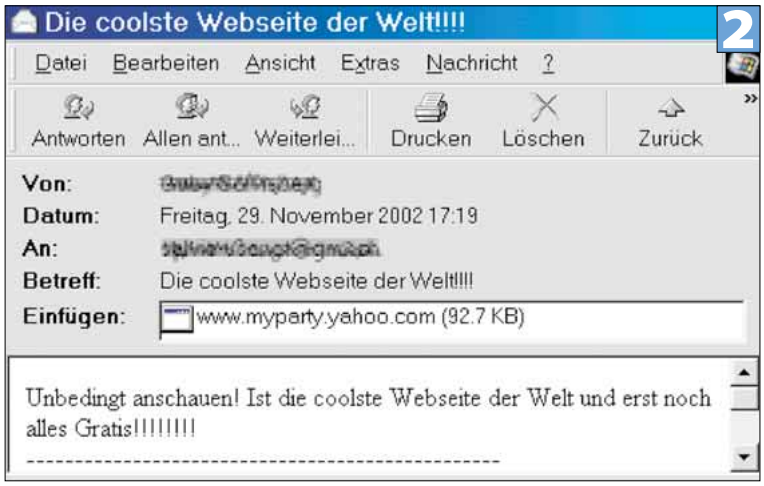
HTA- oder HTML-Code kann sich allerdings hinter jeder beliebigen Endung verstecken, wenn es dem Programmierer gelingt, den Code über einen Link direkt mit dem Browser öffnen zu lassen.

Bei VBS-Dateien vertrauen Virenprogrammierer auf die weit verbreitete Einstellung des Windows-Explorers, um bekannte Endungen auszublenden. Sie nennen dann die schädliche Beilage etwa «Love-Letter-For-You.TXT.VBS» – beim Empfänger bleibt «Love-Letter-ForYou.TXT übrig. Über Extras/Ordneroptionen/Ansicht verbieten Sie dem Windows-Explorer, die Endungen auszublenden: Deaktivieren Sie das Häkchen bei «Dateinamenerweiterung bei bekannten Dateitypen ausblenden», **Screen 3**.

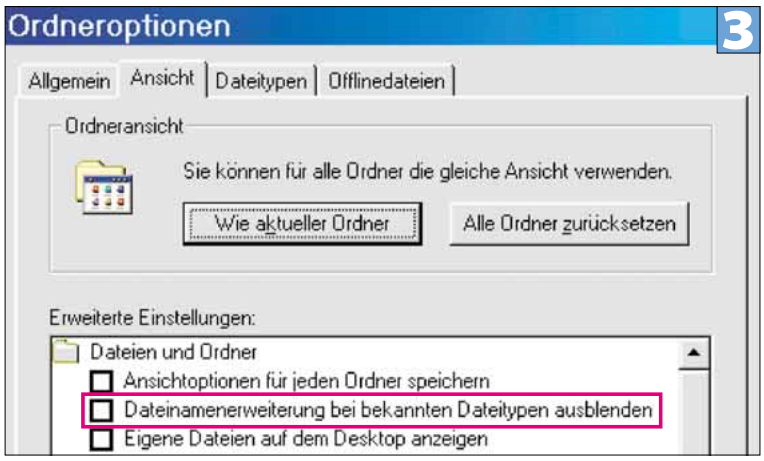
VBA-Makros in Office-Dateien: Die Gefahr durch VBA-Makroviren in DOC-, XLS-, PPT- und MDB-Dateien ist deutlich gesunken, seit Microsoft den Makroviren-Schutz in die Office-Programme integriert hat (zu finden unter Extras/Makro/Sicherheit/Sicherheitsstufe). Die grösste Gefahr in diesem Segment stellen so genannte AutoOpen-Makros dar, die sich beim Öffnen eines Dokuments automatisch ausführen. Je nach verwendeter Sicherheitsstufe ▶



Diese Demodateien sind harmlos und zeigen die im Artikel beschriebenen Phänomene.



Unaufmerksame Benutzer könnten darauf hereinfallen: Die Endung COM ist nicht immer eine Webseite.



Deaktivieren Sie «Dateinamenerweiterung bei bekannten Dateitypen ausblenden», um über versteckte Erweiterungen informiert zu werden.

Fachchinesisch

Code

Code besteht aus Textzeichen, die Anweisungen enthalten, was bei welcher Benutzeraktion zu tun ist. Diesen Text nennt man auch Programmcode oder Quellcode, englisch Source Code. Während der Code von echten Programmen wie Word nicht einsehbar ist, lassen sich Makros und Scripts meist mit Text-Editoren öffnen.

Scripts

Scripts enthalten unterschiedlichste Anweisungen an ein bestimmtes Programm oder ans Betriebssystem und sind sehr stark mit Makros vergleichbar. Scriptsprachen wie z. B. JavaScript oder VisualBasic Script werden oft eingesetzt, um Internetseiten interaktiv zu gestalten.

VBA-Makro

VisualBasic for Applications (VBA) ist die Script-Sprache, die in Microsoft-Office-Programmen (Word, Excel etc.) für Makros verwendet wird. Ein Makro ist eine aufgezeichnete oder manuell programmierte Abfolge von Befehlen an ein Programm. Dank des Makros lassen sich Befehlsfolgen jederzeit automatisch wiederholen.

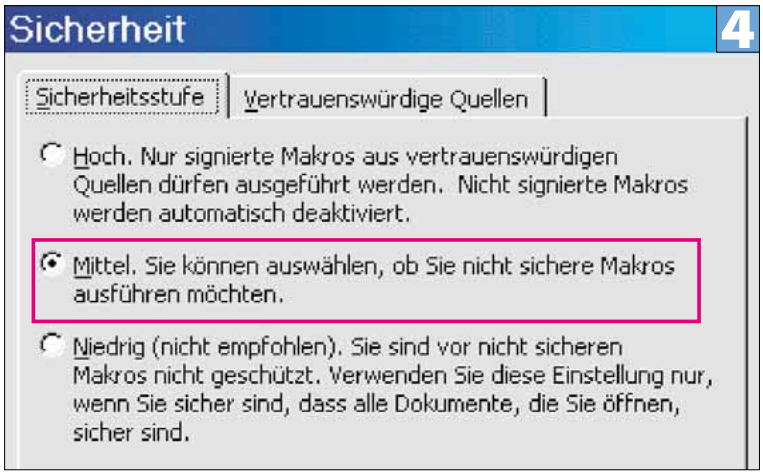
Script-Interpreter

Damit ein Computer die Anweisungen von Scripts versteht, braucht er ein kleines Programm, das sich auf die im Script verwendete Sprache spezialisiert hat und dessen Anweisungen interpretiert – den Interpreter. Der Windows Scripting Host und die Datei COMMAND.COM sind wohl die zwei häufigsten Interpreter unter Windows.

▶ werden solche Makros mit der Einstellung HOCH gar nicht ausgeführt oder mit der Stufe MITTEL erst nach expliziter Erlaubnis des Benutzers, **Screen 4**.

Eine Sicherheitslücke älterer Office-Versionen bestand darin, AutoOpen-Makros über eine verknüpfte Dateivorlage auszuführen und damit den Makro-Schutz zu umgehen. Mit Office 2000 und XP ist dies nicht mehr möglich. Nur in Word darf die Standardvorlage NORMAL.DOT noch den Makroviren-Schutz durchbrechen. Das scheint aber unbedenklich, da die Datei lokal gespeichert ist.

Office-Dateien sind bei aktiviertem Schutz relativ sicher. Es genügt aber schon eine ➔ **Registry**-Veränderung, um zum Beispiel den Makroviren-Schutz in Word auszuhebeln. Allerdings müsste es dem Virenprogrammierer gelingen, zwei Aktionen zu koppeln: Erst mit dem Registry-Import den Schutz abzuschalten und danach Word mit der Makrodatei zu laden. Theoretisch ist das möglich. Praktisch – und Virenprogrammierer denken sehr praktisch – ist es nicht.



Mit Sicherheitsstufe «Mittel» werden Sie vor dem Ausführen eines Makros um Erlaubnis gefragt.

Fachchinesisch

Registry

Spezielle Datenbank, die von Windows verwaltet wird. Auf Grund der Registry weiss Windows, wie gewisse Dateitypen (Dokumente, Kalkulationstabellen usw.) bearbeitet werden müssen.

Seit Office 2000 geniessen Word und Excel einen besonderen Status unter Windows. Bei allen nicht registrierten Endungen sieht der Windows-Explorer nach, ob es sich bei einer Datei um das Word- oder Excel-Format handelt. Ist das der Fall, lädt der Explorer die Datei in der passenden Office-Anwendung. Steht der Makroviren-Schutz auf NIEDRIG, droht somit von jeder beliebigen Fantasie-Endung Gefahr.

Stapelverarbeitungsdateien (BAT, CMD): Batch-Dateien mit der Endung BAT sind einfache Textdateien mit beliebig vielen Kommandos, die nach einem Doppelklick sofort abgearbeitet werden. Ursprünglich waren Batch-Dateien zum Automatisieren umfangreicher Arbeitsschritte

unter DOS gedacht. Ihre Fähigkeiten sind inzwischen jedoch erheblich grösser, da neben den DOS-Standardbefehlen und -Programmen auch Windows-Befehle möglich sind, etwa zum Importieren von Registry-Einträgen oder zum Ausführen anderer Programme. Der Doppelklick auf unbekannte BAT-Dateien kann grossen Schaden anrichten, aber auch weniger offensichtliche, dezente Konfigurationsänderungen auslösen.

Für komplexe Viren, die sich weiterverbreiten, reicht die simple Batch-Sprache aber meist nicht aus. Wer Batch-Dateien zu lesen versteht, sollte vor dem Start einer solchen Datei ihren gesamten (!) Inhalt prüfen: Schädliche Kommandos können beispielsweise auch nach hundert Leerzeilen oder in einer scheinbar leeren Zeile nach etlichen Leerzeichen stehen (siehe Box « Aufgedeckt», unten).

Batch-Befehle lassen sich leider ohne grosse Mühe verstecken. In einer Datei «VieleGruesse.DOC», die durchaus normalen Grusstext enthalten kann, befindet sich vielleicht eine Reihe von Kommandos, die mit einem simplen Befehl oder mit einer entsprechend gestalteten Verknüpfung direkt an den so genannten Kommando-Interpreter gesandt werden, der diese Befehle ausführt. Das ist gleichbedeutend mit dem Doppelklick auf eine «VieleGruesse.BAT» gleichen Inhalts.

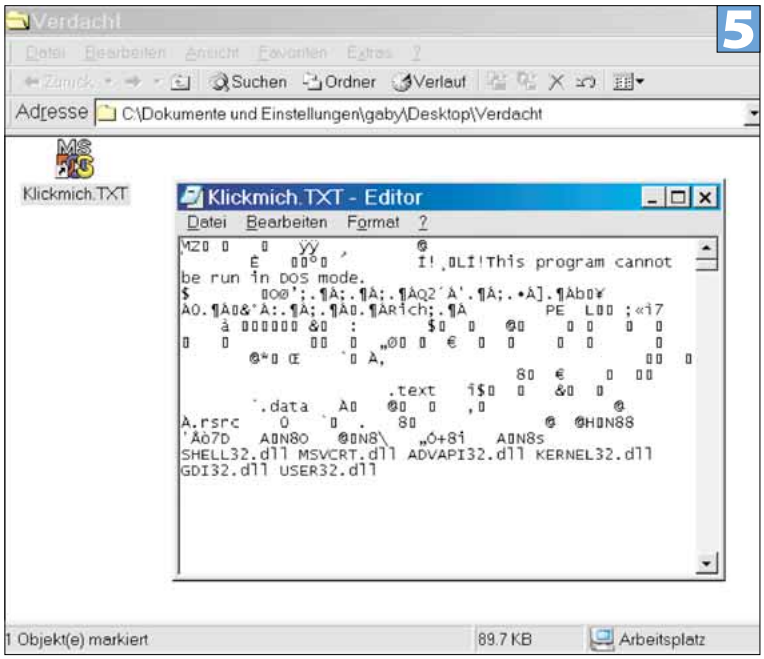
Registry-Import – die Endung REG: Export-/Importdateien für die Registry tragen die Endung REG und sind standardmässig so mit dem Registry-Editor REGEDIT.EXE verknüpft, dass dieser sie beim Doppelklick einliest. Allerdings erscheint vorher ein Abfrage-Dialog, der auf eine Bestätigung des Benutzers wartet. Zudem lassen sich solche REG-Dateien genau wie die BAT-Dateien mit dem Notepad-Editor inspizieren.

Gut getarnte Registry-Eingriffe verlassen sich aber nicht auf den Doppelklick des Anwenders. Die vom Virenprogrammierer gewünschte Registry-Änderung geschieht daher oft per Programm oder Script. Auch der Weg über einen Link verspricht besseren Erfolg, weil dann sowohl die verräterische Endung REG als auch die Sicherheitsabfrage vermieden wird (siehe Abschnitt «Verknüpfungen – LNK, URL, PIF», rechte Spalte). Typisch ist die Methode von Viren, sich in der Registry so einzutragen, dass sie selbst bei jedem Windows-Start automatisch ausgeführt werden. Ebenfalls üblich ist das Abschalten diverser Sicherheitsstandards, um dem Schädling alle Barrieren wegzuräumen. Registry-Eingriffe haben also meist vorbereitenden und begleitenden Charakter.

Notepad-Editor

Aufgedeckt

Viele potenziell gefährliche Dateien (HTML, BAT, diverse Scripts) lassen sich im Notepad-Editor begutachten, weil sie im reinen Textformat geschrieben sind.
Um eine solche Datei gefahrlos zu öffnen, starten Sie zuerst über START/PROGRAMME/ZUBEHÖR den Notepad-Editor, gehen zu DATEI/ÖFFNEN, wählen die fragliche Datei aus und klicken auf OK. Damit wird die Datei nicht ausgeführt, sondern lediglich in reinem Text angezeigt. Wer die verwendete HTML-, Script- oder Batch-Sprache ein wenig versteht, hat dann schon einen guten Überblick darüber, was die Datei mit Ihrem System vorhatte.



5 **Wäre Klickmich.TXT wirklich eine Text-Datei, würde im Notepad kein Zeichensalat erscheinen. Klarer Fall: Es ist ein Programm, also potenziell gefährlich.**

DOC-Auszüge SHS und SHB: Dokumentauszüge (Shellscraps) sind an sich harmlose Textschnipsel: Sie markieren einen Teil einer Word-Datei und ziehen ihn auf den Desktop oder in ein Windows-Explorer-Fenster. Damit ersparen Sie sich, für den Textteil in Word eine separate Datei anzulegen. Leider bergen solche Auszüge ein Sicherheitsrisiko. Es ist nämlich ebenso gut möglich, in Word ein «Paket» (EINFÜGEN/OBJEKT/PAKET) mit DOS- oder Windows-Befehlszeilen anzulegen und dann dieses Paket als Scrap-Datei mit Endung SHS zu speichern. Das als Datei isolierte Paket sieht aus wie ein harmloser Textauszug, enthält aber einen Schädling. Beim Öffnen eines solchen Pakets in Word werden Sie vor möglichen Risiken gewarnt, jedoch nicht beim Doppelklick einer SHS-Datei im Windows-Explorer.

Dass sich ein ganzer Wurm in SHS-Dateien verstecken lässt, hat «VBS.Stages» (**http://www.pctip.ch/helpdesk/virenticker/archiv/16015.asp**) bewiesen. SHS-Dateien, die Sie nicht selbst erstellt haben, sind hochgradig verdächtig. Verzichten Sie auf das Verwenden von SHS-Dateien und bringen Sie Windows dazu, diese Endungen stets anzuzeigen. Wie dies geht, lesen Sie im Top-Thema vom 22. Juni 2000 auf unserer Webseite (**http://www.pctip.ch/topthema/tt/16050.asp**).

Installations-Scripts – INF-Dateien: INF-Dateien dienen in erster Linie zur Installation von Treibern oder kleinen Programmen. Die Möglichkeiten eines solchen INF-Scripts umfassen das Löschen, Kopieren, Umbenennen von Dateien und vor allem das Ändern von Registry-Einträgen. Die aktuellen Windows-Versionen sind so voreingestellt, dass der Doppelklick auf eine INF-Datei sie wie eine Textdatei im Notepad-Editor öffnet. Der Kontextmenü-Eintrag INSTALLIEREN muss bewusst gewählt oder per Link-Datei erzwungen werden. Das senkt das Risiko der an sich mächtigen Installations-Scripts beträchtlich.

Die Datei AUTORUN.INF, die Sie oft auf CD-ROMs antreffen, hat mit den Installations-Scripts eigentlich nur die Endung gemeinsam. Diese INF-Datei besitzt einen eigenen einfachen Befehlssatz, um der eingelegten CD im Windows-Explorer ein bestimmtes Icon zuzuordnen oder um beim Einlegen der CD automatisch ein bestimmtes Programm zu laden. Damit werden fremde CDs zu einem erheblichen Risiko, da der Hersteller über diese AUTORUN.INF jedes beliebige Script oder Programm der CD starten kann. Wir empfehlen bei häufigem Umgang mit fremden CDs, den Autostart-Mechanismus zu deaktivieren. Nachzulesen in «Windows nervt!» aus dem PCtip 9/2002, S. 37. Sie finden den Artikel auch als PDF-Datei in unserem Archiv (**http://www.pctip.ch/archiv/2002/9.asp**).

Verknüpfungen – LNK, URL, PIF: Im Alltag werden LNK-Dateien erzeugt, wenn Sie etwa eine Verknüpfung einer Datei oder eines Ordners auf Ihrem Windows-Schreibtisch ablegen. URL-Dateien entstehen auf ähnliche Weise, betreffen aber Verknüpfungen zu Webseiten. Vor allem die Verknüpfungsdateien LNK, URL und PIF scheinen auf den ersten Blick harmlos und verweisen normalerweise auf eine weitere Datei oder Adresse. Angesichts ihrer zahlreichen Tarnmöglichkeiten sind solche Verknüpfungen jedoch manchmal trotzdem gefährlich. ▶

▶ Eine manipulierte LNK-Datei kann im Hintergrund Informationen aus einer harmlos aussehenden Datei mit beliebiger Endung in die Registry eintragen – vorausgesetzt, es handelt sich dabei in Wirklichkeit um eine REG-Datei. Analog kann eine Verknüpfungs-Datei HTA-Code direkt dem Browser übergeben oder Batchbefehle an den Kommando-Interpreter leiten.

Kommt hinzu, dass LNK-, PIF- und URL-Dateien jedes schmucke Icon tragen dürfen und ihre Endung grundsätzlich verbergen. Sie können also durchaus als z. B. «Klickmich.TXT» erscheinen. Hier lauern zahllose Verstecke und psychologische Tricks, **Screen 5**, Seite 27.

Als besonders irreführend kann sich die Verknüpfung vom Typ URL erweisen: Es muss sich keineswegs um eine echte «Internetverknüpfung» handeln. Klicken Sie mit Rechts auf eine URL-Datei und wählen Sie EIGENSCHAFTEN. Ist dort als URL der Eintrag «file:///» mit nachfolgendem lokalen Pfad oder Netzpfad angegeben, verweist die URL-Datei vielleicht auf ein fatales Programm mit der Endung EXE, das Sie nie direkt anklicken würden. Wenn Sie sich nicht sicher sind, ob Sie die Verknüpfung selbst erstellt haben, schauen Sie sich stets deren Eigenschaften an, um herauszufinden, wohin sie verlinken will, **Screen 6**.

URL-Dateien können auch auf lokal installierte Programme verweisen, wie hier auf den Internet Explorer.

Theoretische Gefahren

CHM-Dateien sind das aktuelle Format für Windows-Hilfedateien. Über interne Links können sie externen ausführbaren Code aufrufen. Ein seltenes Beispiel für eine schädliche CHM-Beilage war der «BleBla»-Wurm: **http://www.pctip.ch/helpdesk/virenticker/archiv/17246.asp**.

ISP-Dateien sind einfache Text-Scripts für das Konfigurieren von Internetverbindungen. Sie kamen vor einigen Jahren in Verruf, als eine Sicherheitslücke des Internet Explorers 3.0 den Aufruf von beliebigen DOS- oder Windows-Programmen zuliess. Aktuelle Sicherheitsrisiken sind jedoch nicht bekannt.

Hintergrund

Die Unterschiede

Alle schädlichen Programme sind lästig und potenziell gefährlich. Doch worin unterscheiden sie sich?

Trojaner: **Bei den «trojanischen Pferden» handelt es sich um unerwünschte Software mit einem für den PC oder die Benutzerdaten schädlichen Verhalten. Trojaner geben meist vor, etwas anderes zu sein, z. B. ein nützliches Hilfsprogramm. Trojaner verbreiten sich nicht von selbst und stecken keine bestehenden Dateien an.**

Würmer: **Ein Trojaner plus eine automatische Weiterverbreitungsfunktion ergibt sozusagen einen Wurm. Würmer stecken in der Regel ebenfalls keine bestehenden Dateien an.**

Viren: **Im Gegensatz zu Trojanern und Würmern können Viren bestehende Dateien (Programme, Office-Dokumente) anstecken, sodass diese danach den Virus in sich tragen.**

PDF-Dateien sind grundsätzlich unbedenklich, sofern Sie nur den Acrobat Reader benutzen, um sie anzuzeigen. Eine theoretische Gefahr besteht nur mit dem Adobe Distiller zum Erstellen von PDF-Dateien. Im Sommer 2001 tauchte als «Machbarkeitsbeweis» ein Wurm namens Peachy (**http://www.pctip.ch/webnews/wn/19064.asp**) auf, der jedoch wegen der relativ geringen Dichte an Distiller-Besitzern nur wenige Computer befiel.

SCF-Scripts enthalten simple Befehle im reinen Textformat für den Windows-Explorer. Es besteht ein geringes Risiko, dass diese SCF-Dateien undokumentierte und bislang unbekannte Befehle erlauben könnten.

Sonstige Dateitypen: Viren in RTF-Dokumenten, Bild- oder Musikdateien können Sie derzeit ebenfalls der Kategorie ungefährlicher Laborversuche zurechnen. Virenprogrammierer wollen schliesslich zählbaren Erfolg, und der ist nur über Standardmechanismen zu erzielen. Unter normalen Bedingungen sind diese Formate allesamt sicher.

Minimieren Sie die Risiken: Weder beim Mailen noch bei der Arbeit im lokalen Netz oder im Internet wäre die generelle Empfehlung realistisch, allen hier beschriebenen Dateitypen rigoros aus dem Weg zu gehen. Nehmen Sie sich aber stets die Zeit, Herkunft und Eigenschaften einer Datei genau anzusehen, bevor Sie sie starten.

Für Mails gilt: Erhalten Sie eine persönliche Mail eines Bekannten, der in einem zu ihm passenden Sprachstil schreibt und im Mailtext auf eine Beilage mit einem bestimmten Dateinamen und Inhalt verweist, dann können Sie der Datei so weit vertrauen, wie Sie dem Absender vertrauen.

Ist der Mailtext zwar persönlich, ohne aber auf den Anhang zu verweisen, könnte der Anhang ohne Wissen des Absenders mitgesendet worden sein. In diesem Fall sollten Sie nachfragen. Das Gleiche gilt, wenn Sie eine leere Mail oder einen unpersönlichen Text mit Beilage von einem Bekannten erhalten. Unpersönlichen Mails mit irgendwelchen Angeboten und Versprechungen sollten Sie immer misstrauen, selbst wenn es sich scheinbar um einen bekannten Absender handelt, etwa eine grosse Firma. Solche Absender-Mailadressen können gefälscht sein.

Natürlich wird Ihre Virenscanner-Software jetzt nicht überflüssig. Vier Augen sehen bekanntlich mehr als zwei (siehe «Wie scanne ich eine Mailbeilage nach Viren», S. 63). Virenscanner müssen durch regelmässige Updates gepflegt werden, um neue Viren aufzuspüren. Einer neuen Bedrohung hinken die Antiviren-Hersteller jedoch immer mindestens um einen halben bis ganzen Tag hinterher. Das Wissen um die Dateitypen kann für Ihr System daher die Rettung bedeuten, falls Sie zu den Ersten gehören, in deren Postfach ein brandneuer Schädling landet.