Ungebetene Gäste: TROJANER AM WINDOWS-PC

Das Thema Systemsicherheit betrifft selbstverständlich alle Betriebssysteme – bei MS-Windows entwickelt es sich jedoch zu einem Dauerbrenner: Beinahe täglich werden neue Sicherheitslücken entdeckt, die immer wieder die Endanwender betreffen. Die Firma Microsoft vertritt derzeit die Philosophie, alle ihr bekannt gewordenen Sicherheitsprobleme jeden zweiten Dienstag im Monat zu veröffentlichen. Meistens ist es dann nur mehr eine Frage der Zeit, bis ein Virus, Wurm oder Trojaner im Netz auftaucht, der die Sicherheitslücke für seine Zwecke ausnutzt.

Böse Software

Unerwünschte, schädliche und/oder sich selbst verbreitende Programme werden als *Malicious Software* (kurz *Malware*) bezeichnet. Im wesentlichen unterscheidet man dabei drei Kategorien:

- Ein **Virus** ist ein selbstreplizierendes Programm, das in der Regel auf dem befallenen Rechner verschiedene Störaktionen ausführt. Bis zum Auslösen dieser Störaktionen agiert das Virus meist ohne Wissen des Benutzers. Viren verbreiten sich passiv auf lokalen Systemen (Festplatten und Windows-Shares): Sie infizieren intakte Anwendungsprogramme, indem sie ihren eigenen Programmcode in deren Befehlskette einschleusen. Beim Starten der Anwendung wird dann vorher das Virus ausgeführt.

- Ein **Wurm** kopiert sich selbsttätig über das Netzwerk auf andere Rechner weiter, wobei er oft bestehende Sicherheitslücken ausnutzt. Im Unterschied zu Viren vermehren sich Würmer nicht über Wirtsprogramme, sondern schreiben üblicherweise neue Dateien auf die Festplatte des Opfers oder ersetzen vorhandene Dateien. Eine große Gefahr von Wurmattacken liegt in ihrer enormen Verbreitungsgeschwindigkeit und der daraus resultierenden Netzbelastung: Innerhalb weniger Minuten können dadurch ganze Netzwerke bzw. sogar große Teile des Internet lahm gelegt werden.

- Ein **Trojanisches Pferd** (kurz, wenn auch nicht ganz korrekt: Trojaner) ist per Definition eine Software, die auf dem Rechner eines Benutzers ohne dessen Wissen als Agent eines Angreifers agiert, also im Prinzip jedes Programm mit einer verborgenen Absicht. Trojanische Pferde geben häufig vor, etwas Nützliches zu tun bzw. tun dies wirklich; gleichzeitig führen sie aber auch unerwünschte Aktionen aus – vom Ausspähen der Benutzerdaten und Passwörter bis zur totalen Übernahme des Systems. Trojaner verbreiten sich in der Regel nicht aktiv weiter, sondern werden entweder von Hackern gezielt eingeschleust oder vom Benutzer „eingeladen“: beispielsweise durch das Öffnen von eMail-Attachments, durch Mausklicks auf aktive Web-Inhalte oder durch die Installation verseuchter Freeware- oder Shareware-Programme.

Die Grenze zwischen den verschiedenen Schädlingen ist fließend – Viren und Würmer können auch Trojanerfunktionen mit übertragen. Ein Trojanisches Pferd kann also zum Beispiel durch ein Virus, einen Wurm, ein eMail-Attachment, einen Hacker und sogar durch Zustimmung des Benutzers in das System gelangen. Die Vielfalt der Ausbreitungsmethoden und versteckten Tätigkeiten von Trojanern ist bedrückend.

Wer ist der Feind?

Trojanische Pferde sind ein bunter Haufen: Es gibt unter anderem Adware, Spyware, Trickleware, Browser Helper Objects, RATs, Rootkits, Key Logger, Hijacker, Dialer, Dropper, Loader, Binder und Nuker. Trojaner können den ahnungslosen Benutzer ausspähen, sein Verhalten analysieren, Tastatureingaben mitlesen, ihm bestimmte Informationen aufdrängen, sensible Daten an Dritte weiterleiten und sogar Hintertüren für Hacker öffnen, indem sie den Zugriff von außen auf den Rechner über bestimmte Ports erlauben.

Berüchtigt sind z.B. die so genannten Dialer, die Internetverbindungen über die Telefonleitung aufbauen – und mitunter statt der vom Benutzer vorgesehenen Nummer teure 0900- oder 01900-Nummern anwählen. Einen Dialer erhält man oft durch einen unbedachten Mausklick im Browser. Andere Trojaner tarnen sich, indem sie sich als hilfreiche Zusatzprogramme ausgeben oder sich – wie Rootkits – den Augen des Benutzers überhaupt entziehen.

Adware

Als Adware bezeichnet man Programme, die angeblich nützliche Extrafunktionen bringen und nur mit expliziter Zustimmung des Benutzers installiert werden. Zu dieser Gruppe gehören auch die so genannten „Download-Beschleuniger“ – die tatsächlich Download-Bremsen sind, da sie für Abfragen und Informationen des Werbeträgers einen guten Teil der vorhandenen Bandbreite verbrauchen.

Adware registriert oft die persönlichen Daten und Gewohnheiten des Benutzers und sendet diese an einen zentralen Server. Der Benutzer kann sich dagegen rechtlich kaum zur Wehr setzen – schließlich hat er bei der Installation ausdrücklich der Informationspolitik (*Policy*) des Werbeträgers zugestimmt bzw. wurde informiert, wo er diese im WWW nachlesen kann.

Beispielsweise wird derzeit bei vielen Versionen des *Peer-to-Peer* (P2P)-Programms KaZaa (siehe *Freeware und Shareware*, Seite 13) die Adware Bullguard mitgeliefert: Bullguard ist ein so genannter Data Miner, der unter anderem den Namen des Benutzers, seine eMail-Adresse, Informationen über die auf dem PC installierten Anwendungen sowie Kreditkarteninformationen sammelt und an Tochterfirmen, Geschäftspartner usw. des Herstellers weiterleitet. Dies ist im *End-User License Agreement* von Bullguard explizit angeführt; auf der Webseite von Bullguard erfährt man, dass die Offenlegung der Policy nur zur Information des Benutzers dient und dass dieser keinerlei Anspruch darauf hat, dass

Alarmstufe Rot: Rootkits

Rootkits sind die mächtigsten und tückischsten aller Trojaner: Diese Software-Werkzeuge (*Kits*) verschaffen dem Angreifer alle Rechte des Administrators (unter Unix *Root* genannt) und somit volle Kontrolle über das befallene System. Zusätzlich sind sie in der Lage, ihre Existenz durch gefinkelte Mechanismen nahezu perfekt zu verschleiern. Ein Rootkit ist daher der ultimative Schrecken jedes Systemverantwortlichen.

Während Rootkits in der Unix-Welt schon lange ein Problem darstellen, sind Windows-Rootkits relativ neu: 1999 wurde erstmals gezeigt, dass es technisch möglich ist, in den Betriebssystem-Kern von MS-Windows einen Trojaner einzubauen. Ein Angriff auf dieser Ebene umgeht sämtliche Sicherheitsvorkehrungen des Systems. Windows-Rootkits – die glücklicherweise derzeit noch eher selten anzutreffen sind – verstecken sich gern in DLLs (*Dynamic Link Libraries*) oder tarnen sich als Gerätetreiber. Sie setzen üblicherweise bei den Schnittstellen zwischen Anwendungsprogrammen und Betriebssystem-Kern (*Application Programming Interfaces*, kurz APIs) an und filtern jede Kommunikation zwischen der Anwendung und dem Betriebssystem. An dieser Stelle kann der Angreifer den Datenfluss manipulieren und somit dem ahnungslosen Administrator eine heile Welt vorgaukeln. Auch der Systemleerlauf-Prozess, der immer dann aktiv ist, wenn der Windows-PC nichts zu tun hat, ist ein ideales Versteck für Rootkits: Dadurch, dass der Trojaner nur bei Leerlauf tätig wird, bleiben allfällige Performance-Einbußen aufgrund verborgener Aktivitäten garantiert unbemerkt.

Rootkits bestehen typischerweise aus mehreren Komponenten:

- Die „Hintertür" (*Backdoor*) für den Angreifer sichert diesem uneingeschränkten Zugang zum System – unter Windows als Administrator. Gängige Backdoor-Methoden sind z.B. bestimmte Benutzername-/Kennwort-Kombinationen zur Autorisierung gegenüber einem Service des Systems oder zusätzliche Programme, die dem Angreifer volle Rechte erteilen.
- Die Trojaner-Komponente stellt sicher, dass alle zum Rootkit gehörigen Dateien sowie die anfallenden Daten unsichtbar bleiben. Zu diesem Zweck kann der Trojaner sogar die Systemereignis-Protokolle (*Logfiles*) bzw. den Windows Task-Manager manipulieren. Meistens ist dies jedoch überflüssig: Programme, die der Hacker für seine Schandtaten benötigt, werden normalerweise bei ihrer Ausführung gar nicht erst angezeigt. Der echte Administrator sieht in der Systemanzeige von den verdeckt durchgeführten Aktionen in der Regel nichts – und wenn er zufällig doch einmal einen *Process Identifier* (PID) des Trojaners entdeckt, bleibt jeder Versuch, diese Anwendung zu stoppen, erfolglos.
- Oft sind auch Key Logger oder Packet Sniffer integriert, um weitere Benutzerberechtigungen auszuspähen.
- Zu guter Letzt wird meist noch die ursprüngliche Lücke geschlossen, durch die der Angreifer ins System kam: So kann ihm kein anderer Hacker den übernommenen Rechner streitig machen.

Ist ein Rootkit erst einmal installiert, wird es schwierig. Handelsübliche Virenscanner versagen – sie können nur auf der Programmebene suchen und müssen sich darauf verlassen, dass das Dateisystem ihnen vollen Zugang zu allen Daten gewährt. Ein Scanprogramm für Rootkits muss aber den Betriebssystem-Kern durchsuchen und darf sich auf nichts verlassen: Da ein Rootkit imstande ist, die Ausführung eines Programms auf beliebige andere umzuleiten, kann es sogar die korrekte Ausführung des Scanprogramms unterbinden.

Ein Virenscanner hat gegen ein Rootkit nur dann eine Chance, wenn es ihm gelingt, eine Signatur des Trojaners vor dessen Installation zu erkennen und sein Einnisten zu verhindern. Daher ist der ununterbrochene Betrieb eines Virenscanners mit stets aktueller Virendatenbank die beste Vorbeugungsmaßnahme gegen Windows-Rootkits. Weitere Informationen zu diesem Thema finden Sie unter `http://www.rootkit.com/`.

die Firma sich daran hält. Zur Ehrenrettung von Bullguard sei gesagt, dass dies durchaus branchenüblich ist.

Eine extreme Verbreitung erlebt derzeit die Adware StopSign, die „huckepack" mit mehreren P2P-Programmen mitkommt. StopSign dient als Träger für Werbeeinschaltungen; nebenbei stoppt es verschiedene Security-Programme (Firewalls, Virenscanner) auf dem Rechner des Opfers. Wenn es dazu selbst nicht in der Lage ist, wird der Benutzer aufgefordert, dies zu tun – mit durchaus plausibel klingenden Anfragen: Beispielsweise schlägt die Software vor, das Programm Norton Antivirus temporär abzuschalten, weil ein „Initialisierungskonflikt" bei der Installation von StopSign besteht. StopSign wird beim Starten des Rechners in dessen Arbeitsspeicher geladen und bleibt dadurch selbst nach der Entfernung des Programms noch aktiv. Darüber hinaus ist StopSign ein so genannter Loader, d.h. es lädt, installiert und startet heimlich weitere Programme auf dem PC des Opfers. Installiert der Benutzer bestimmte Personal Firewalls (Sygate, ZoneAlarm) nach StopSign, können die betroffenen PCs nicht mehr starten.

Spyware

Spyware funktioniert ähnlich wie Adware, allerdings mit zwei gravierenden Unterschieden: Zum einen wird der Benutzer über die Präsenz des Trojaners nicht informiert, zum anderen kann dieser auch durch eine Deinstallation der jeweiligen Trägersoftware (z.B. KaZaa) nicht entfernt oder gestoppt werden.

Sehr verbreitet ist beispielsweise Aureate/Radiate – eine Spyware, die mit Freeware-Virenscannern, Bildschirmschonern, Spielen, HTML-Convertern, ZIP-Software, Callcenter-Software usw. „frei Haus" geliefert wird. Aureate informiert seine zentralen Server zunächst über den Benutzer des bespitzelten PCs: Sein Name, seine Internetadresse und eine Liste aller installierten Softwareprodukte werden aus dem PC ausgelesen und weitergeleitet. Anschließend wird den Aureate-Servern über jede Browseraktivität und alle Datei-Downloads berichtet; wenn der Benutzer einen Modemzugang verwendet, werden auch die Telefonnummer des Providers und das Zugangspasswort übermittelt.

Ein häufig anzutreffender Vertreter der Spyware ist auch der BDE Projector, der sich oft als Anhängsel von P2P-Software auf dem Rechner einnistet (z.B. war er Teil älterer KaZaa-Versionen). „Im Interesse des Anwenders", der mit diesem Werkzeug alle Arten von digitalen Medien suchen, erhalten und wiedergeben kann, verfolgt die Software jede Aktion des Benutzers und des Browsers und berichtet darüber einem zentralen Server. Der BDE Projector lädt Updates und andere Programme aus dem Internet, ohne den Benutzer darüber zu informieren. Da er diese Software nur auf dem PC ablegt, ohne sie zu starten, ist er zur Klasse der Dropper zu zählen. Nebst allen anderen Übeln bewirkt der BDE Projector aufgrund seiner engen Verknüpfung mit Grafikbeschleunigern und Musikwiedergabefunktionen im Betriebssystem auch oft Systemabstürze oder starke Performance-Einbußen.

Die „Elite" unter der Spyware ist die so genannte Trickleware: Diese spioniert ebenfalls persönliche Informationen und Gewohnheiten des Anwenders aus, tarnt ihre Präsenz im System aber zusätzlich durch sehr geschicktes Timing der Datenübermittlung an die zentralen Server.

Browser Helper Objects

Browser Helper Objects (BHOs) sind Programme, die innerhalb des Webbrowsers aktiv sind. Dadurch sitzen sie sozusagen „an der Datenquelle" und wissen über jede aufgerufene Webseite Bescheid. Der Erfinder dieser Softwaretechnik ist Microsoft: BHOs sollten ursprünglich dazu dienen, Webseiten mit unerwünschtem Inhalt für Kinder zu sperren.

Ein verbreitetes BHO ist HotBar, das oft bei iMesh beigepackt ist bzw. sich per eMail als vermeintliches Outlook-Update zu verbreiten versucht. HotBar „befällt" sowohl den Internet Explorer als auch MS-Outlook. Der Benutzer wird zwar gefragt, ob er HotBar installieren will; jedoch führt auch eine Ablehnung zu einer teilweisen Installation der Software. Aus dem *SignUp*-Fenster erfährt HotBar neben Name, Telefonnummer, Anschrift, Mailadresse und Geburtstag des Benutzers auch sein Arbeitsgebiet. Der Internet Explorer erhält durch zusätzliche Schaltleisten ein neues Aussehen.

BHOs haben volle Kontrolle über den Browser. Auch ActiveX-Applets, die der Browser – oft vom Benutzer unbemerkt – über eine Webseite lädt, können BHOs sein. Eine besonders bösartige Variante davon sind die so genannten Hijacker: Sie bewirken, dass der Benutzer manche Seiten nicht mehr ansteuern kann, oder sie verbinden ihn stur nur mehr mit einer bestimmten Werbeseite.

Viele Wege führen nach Troja

Neben eMail gibt es heute für Trojaner vor allem drei Verbreitungswege: Sicherheitslücken des Betriebssystems, Freeware- und Shareware-Programme mit „Nebenwirkungen" sowie aktive Web-Inhalte, die durch allzu sorgloses Surfen im Internet auf den Rechner gelangen.

Sicherheitslücken

Sicherheitslöcher in Betriebssystemen entstehen üblicherweise durch mangelnde Sorgfalt des Herstellers; die häufigsten Ursachen sind Designfehler der Software oder Schlampigkeitsfehler im Code – meist bedingt durch die weit verbreitete „Featuritis" (der Zwang, bei jeder Version einer Software einige neue Funktionen anzubieten) und den enormen Zeitdruck in der IT-Branche. Der Programmcode von MS-Windows umfasst mehrere Millionen Zeilen, sodass die Existenz zahlreicher Sicherheitslücken nicht verwunderlich ist.

Eine Sicherheitslücke wird oft durch Zufall gefunden. Glücklicherweise ist es meistens der Softwarehersteller selbst, der bei seinen Weiterentwicklungen den Fehler entdeckt, ihn korrigiert und eine entsprechende Softwarekorrektur (*Secu-*

rity Patch) im Internet zur Verfügung stellt. Spätestens ab diesem Zeitpunkt wissen auch Hacker über die Sicherheitslücke Bescheid; daher ist es extrem wichtig, vorhandene Security Patches umgehend zu installieren (idealerweise mit Hilfe der Funktion *Automatische Updates*; siehe Seite 18).

Als Beispiel für die nachhaltige Verheerung, die Sicherheitslücken auslösen können, sei der MS-Blaster-Wurm genannt, der sich seit August 2003 von Windows-PC zu Windows-PC fortpflanzt, indem er ein bekanntes Sicherheitsproblem ausnutzt. Zwar gab es beim ersten Auftreten des Wurms längst einen entsprechenden Patch von Microsoft; viele Windows-Benutzer hatten diesen jedoch nicht bzw. nur in einer fehlerhaften Version installiert (Microsoft konnte das Problem erst im zweiten Anlauf vollständig beheben). MS-Blaster verbreitete sich entsprechend rasant. Parallel dazu beobachteten zahlreiche Netzwerkadministratoren massive Scans nach einem bestimmten geöffneten Port auf allen Rechnern mit Internetanschluss. Bald war klar: Im Wurm steckte ein *Remote Access Trojan* (RAT), der auf unzähligen infizierten Rechnern einen Administrator-Zugang von außen über Port 4444 öffnete – die Hacker mussten die befallenen Rechner nur noch mittels Portscans ausfindig machen.

Auch der Bugbear-Wurm, der seit Herbst 2002 bekannt ist und sich über eMail und Netzwerkfreigaben (Windows-Shares) verbreitet, ist ein RAT. Via eMail nutzt er eine Sicherheitslücke in MS-Outlook bzw. Outlook Express und wird sofort aktiv, wenn die Nachricht gelesen wird bzw. die Vorschaufunktion aktiviert ist. Der Wurm öffnet ein bestimmtes Port für den Zugang von außen und beendet jede ihm bekannte Antiviren- und Firewall-Software. Zusätzlich installiert er einen so genannten Key Logger (ein Programm, das Passwörter sammelt) und sendet an alle freigegebenen Netzwerkdrucker unsinnige Druckaufträge, sodass es auch zu einer Blockade von Druckern kommen kann. Die Präsenz eines Bugbear-Wurms ist für aufmerksame Benutzer daran erkennbar, dass im Infobereich der Taskleiste ein durchgestrichenes Programmsymbol erscheint (siehe Abb. 1), wenn eine vorhandene Antiviren-Software bzw. Personal Firewall plötzlich gestoppt wird.

Abb. 1: Infobereich mit gestoppter Personal Firewall (Windows XP)

Freeware und Shareware

Während Sicherheitslöcher im Betriebssystem dem Hersteller angekreidet werden können, ist in den meisten anderen Fällen der Benutzer durch sein Verhalten selbst schuld an der Misere. Ein besonders häufiger Fehler ist das oft zu vertrauensselige Installieren (häufig sogar als Administrator!) von unbekannten Freeware- oder Shareware-Programmen. Viele davon sind jedoch nur deshalb so „kostengünstig", weil sich der Entwickler seinen Lohn noch von einer dritten Stelle holt – z.B. indem er dem Produkt Adware oder Spyware beipackt, die dann Werbefirmen gezielt über die Vorlieben des Opfers informiert.

Ein besonders bequemer Ausbreitungsweg für binäres Ungeziefer sind *Peer-to-Peer* (P2P)-Programme, also z.B. Austauschbörsen wie KaZaa oder Morpheus. Damit lässt sich jede Firewall umgehen, die den Benutzer nicht auf ganz wenige Systeme außerhalb der eigenen Organisation einschränkt. P2P-Programme sind das internetweite Analogon zu Netzwerklaufwerken (Windows-Shares): So wie die Verbreitung von Viren über Netzwerklaufwerke eine Gefahr für einzelne vernetzte PCs darstellt, werden P2P-Mechanismen zum weltweiten Träger von Malware aller Art. Die für P2P-Programme freigegebene Festplattenkapazität von Anwender-PCs (die als verteilter Speicher für die auszutauschenden Objekte verwendet wird) ist heute der größte vernetzte Speicherplatz der Welt. Da der Benutzer praktisch keine Kontrolle über die dort abgelegten Daten hat, sammeln sich in diesen Festplattenbereichen alle möglichen Inhalte – Programme oder Dateien mit kriminellem Inhalt können hier genauso verteilt werden wie Musik oder Videos. Der vor kurzem ausgebrochene Wurm MyDoom/Novarg verwendet z.B. auch die Speicherbereiche von KaZaa zur Verbreitung.

Aktive Web-Inhalte

Über das WWW kann man bösartige Software ebenfalls wunderbar verteilen; vor allem Microsofts ActiveX und die berüchtigten (beim Internet Explorer mittlerweile innerhalb des ActiveX-Kontextes laufenden) Java-Applets sind aufgrund ihrer diversen Sicherheitslücken bei Designern von Malware sehr beliebt. Auch der Internet Explorer selbst steht immer wieder wegen Security-Problemen in den Schlagzeilen – eine seiner zuletzt entdeckten Sicherheitslücken ermöglichte es Betreibern einschlägiger Webseiten, Software ohne Rückfrage auf den PCs der Besucher zu installieren und zu starten. Beim Internet Explorer sollte man daher besonders auf dessen Sicherheitseinstellungen achten und diese von Zeit zu Zeit auch verifizieren. Wer sein Risiko reduzieren will, verwendet aber sinnvollerweise einen anderen Browser: Zwar haben auch Netscape, Mozilla, Opera usw. immer wieder Sicherheitsprobleme, aber bei weitem nicht so oft wie der Internet Explorer.

Ein weiterer Risikofaktor sind Sicherheitslöcher in der Webserver-Software, die ebenfalls schon so manchen Wurm (z.B. Code Red, Nimda) möglich gemacht haben. Wenn Sie auf Ihrem Rechner einen Webserver betreiben, sollten Sie daher unbedingt darauf achten, das System im Hinblick auf Security Patches stets aktuell zu halten.

Hilfe – ein Hacker!

Adware und Spyware verfolgen in der Regel hauptsächlich kommerzielle Ziele und richten daher im allgemeinen etwas weniger Schaden an als andere Trojaner (insbesondere Rootkits), die den kriminellen Zwecken von Hackern dienen. Leider ist die Uni Wien für die meisten Hacker durchaus interessant – allerdings weniger wegen ihrer Daten als aufgrund ihres Netzwerkstandorts: Da das Datennetz der Universität über eine relativ hohe internationale Bandbreite

verfügt, kann eine von ihm ausgehende Störaktion im Netz großen Schaden anrichten.

Der Angriffszyklus eines Hackers verläuft dabei fast immer nach demselben Schema:

- Zuerst durchsucht der Hacker mittels so genannter Portscans das Netz nach Rechnern, die offene Ports und damit einen Eingang ins System aufweisen.
- Im nächsten Schritt überprüft er das Betriebssystem der angreifbaren Rechner genauer – und wird bei einem Teil davon zweifellos Angriffspunkte finden.
- Nun bricht er mit einem geeigneten Programm in das System ein. War der Angriff erfolgreich, werden sofort die Spuren vernichtet: Der echte Administrator soll tunlichst keine Möglichkeit zur Rückverfolgung erhalten.
- Im letzten Schritt nistet er sich mittels Trojaner ein und versucht seine Rechte zu halten bzw. auszubauen.
- Von diesem Unterschlupf aus kann er dann wieder von vorne beginnen (Portscans, Schwachstellen identifizieren, Angriff, Einnisten im System) – mit dem zusätzlichen Vorteil, dass die neu dazu gewonnene Ausgangsbasis seine Herkunft verschleiert.

Ungenügend geschützte Systeme stellen daher nicht nur für ihren Besitzer, sondern für alle Internet-BenutzerInnen ein ernsthaftes Risiko dar. Besonders bedenklich ist dabei die Tatsache, dass durch das Internet bösartige Programme aller Art auch in die Hände von Leuten gelangen, die ansonsten von ihrem Wissensstand her gar nicht in der Lage wären, eine vergleichbare Software zu erfinden oder einzusetzen.

Die einzige wirkungsvolle Vorbeugungsmaßnahme besteht aus der (mittlerweile auch von Microsoft aufgegriffenen) Dreier-Kombination aus automatischen Sicherheits-Updates, Virenscanner und Personal Firewall. Extrem wichtig ist diese „Kombi-Abwehr" bei Notebooks, die in verschiedenen Netzwerken verwendet werden und somit ideale Überträger für binäres Ungeziefer aller Art bilden.

Wer suchet, der findet: Trojanerjagd

Für alle: Ad-aware

Das Scanprogramm Ad-aware ist in der Lage, die meisten Trojaner aufzuspüren und auszuschalten. Zu diesem Zweck sucht Ad-aware (im Gegensatz zu Virenscannern) nicht nur in Dateien, sondern auch in der Windows-Systemregistratur (*Registry*) nach problematischen Einträgen. Um Trojanern möglichst wenig Spielraum für Aktivitäten zu geben, muss die Suche regelmäßig durchgeführt werden; angesichts des geringen Zeitaufwands (je nach eingestellter Scan-Genauigkeit etwa eine Minute pro Suchlauf) sollte dies aber kein Problem darstellen.

Ad-aware wird in einer Freeware- und einer kommerziellen Version angeboten. Der Unterschied besteht darin, dass das käufliche Produkt ein Modul namens Ad-watch enthält, das wie ein Virenscanner arbeitet, d.h. Ungeziefer bereits bei seinem Installationsversuch abblockt. Für die Freeware-Version von Ad-aware (die nur vorhandene Trojaner findet) gilt natürlich ebenfalls die oben beschriebene Gefahr unerwünschter Nebenwirkungen. Wir haben Ad-aware 6.0 daher mit allen verfügbaren Mitteln gründlich untersucht. Obwohl keinerlei Auffälligkeiten gefunden werden konnten, bleibt – wie bei jeder Software – ein gewisses Restrisiko, dass das Programm in einer neuen Version neben seinem eigentlichen Aufgabengebiet plötzlich zusätzliche Aktivitäten zeigt.

Die Freeware-Version von Ad-aware ist unter `http://www.lavasoft.de/` (bzw. für Mailbox-BenutzerInnen auch unter `http://swd.univie.ac.at/` als *Gratissoftware*) erhältlich. Für ein wirkungsvolles Eingreifen benötigt Ad-aware analog zu einem Virenscanner nach der Installation (und danach in regelmäßigen Zeitabständen) die jeweils aktuellste Datenbank mit den Signaturen der bekannten Trojaner. Dieses Update wird durch einen Klick auf den Link *Check for updates now* im *Status*-Fenster von Ad-aware durchgeführt (siehe Abb. 2). Bei Verfügbarkeit einer neuen Version der Datenbank muss der Anwender bestätigen, dass er sie downloaden und installieren will, was dann mit wenigen Mausklicks erledigt ist.

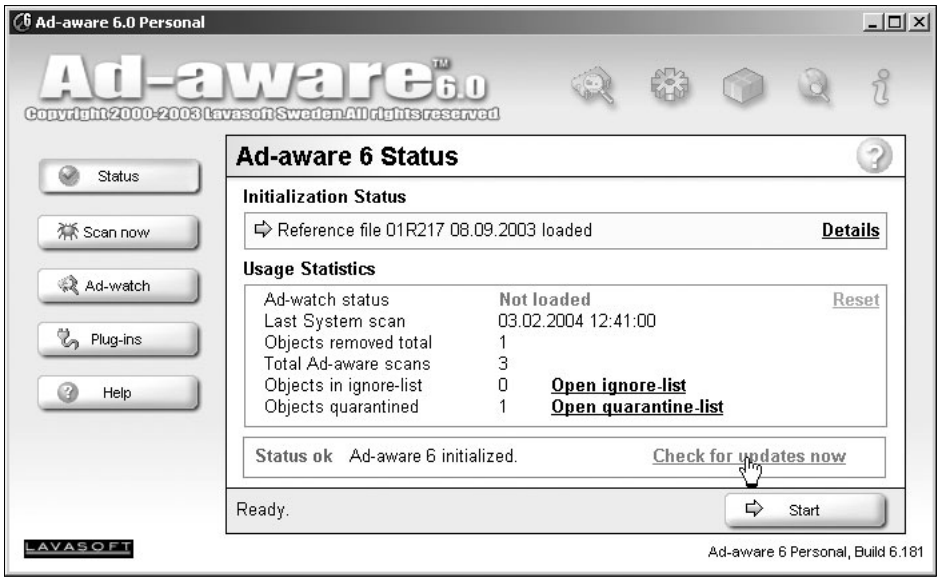

Abb. 2: Ad-aware 6.0 – Fenster *Status*

Der Scan wird durch Anklicken der *Start*-Schaltfläche im *Status*-Fenster in Gang gesetzt. Es erscheint das Fenster *Preparing System Scan*, in

dem Sie den Scan-Modus einstellen können. Die erste, voreingestellte Option *Perform smart system-scan* ist ein durchaus vernünftiger Kompromiss zwischen kurzer Laufzeit und ausreichender Genauigkeit des Scans und kann für den Alltagsgebrauch ruhigen Gewissens verwendet werden. Es empfiehlt sich aber, mindestens einmal wöchentlich einen kompletten Scan über alle Laufwerke vorzunehmen. Wählen Sie dazu im Fenster *Preparing System Scan* die Option *Select drives/folders to scan* und definieren Sie die zu scannenden Laufwerke durch einen Klick in das entsprechende Kontrollkästchen.

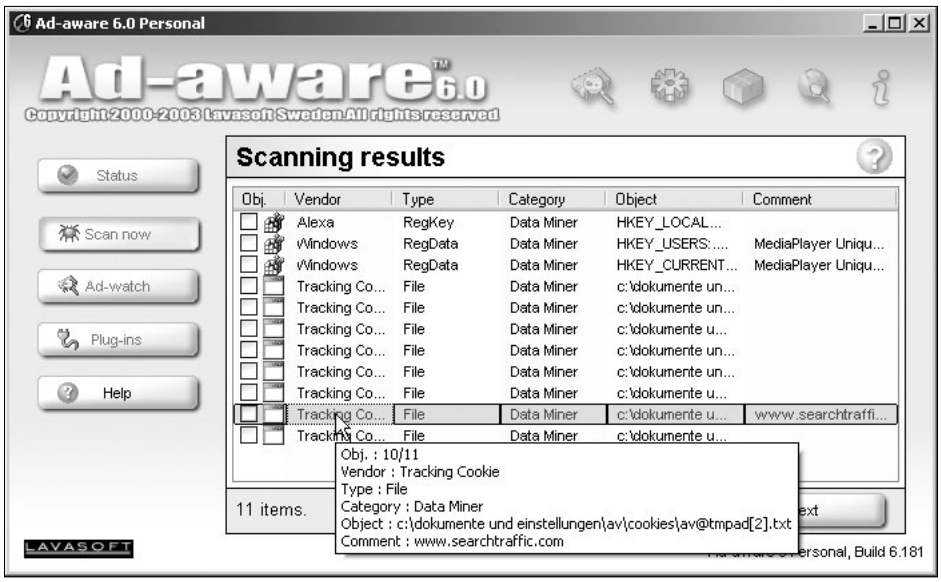

Abb. 3: Ad-aware 6.0 – Fenster *Scanning results*

Der Suchvorgang selbst verläuft wie bei einem herkömmlichen Virenscanner. Ist er abgeschlossen, erhält man eine kurze Zusammenfassung der Ergebnisse; anschließend sollte man sich durch einen Klick auf die Schaltfläche *Show Logfile* (links unten im Ergebnis-Fenster) die Treffer etwas genauer ansehen.

Das Logfile zeigt zuerst jedes im System derzeit laufende Programm (jeden aktiven Prozess) unter Angabe seiner Herkunft, sodass sich Programme unklarer Herkunft identifizieren lassen. Anschließend werden alle Objekte angeführt, die der Klasse des binären Ungeziefers angehören. Durch einen Klick auf die Schaltfläche *Next* werden in einer kurzen Zusammenfassung alle „verdächtigen" Systemeinträge angezeigt (siehe Abb. 3). Aktivieren Sie das Kontrollkästchen ganz links, um ein Objekt für das Entfernen durch Ad-aware freizugeben.

Drei Objekte, die von Microsoft selbst stammen, finden sich auf fast jedem Windows-Rechner: Der Alexa Data Miner (Spyware) ist für die *What's Related*-Links des Internet Explorer verantwortlich. Alexa verfolgt Ihre Gewohnheiten beim Surfen im Netz, um Ihnen Links anzeigen zu können, die Sie vermutlich interessieren. Ein weiterer „MS-Trojaner" ist der MediaPlayer (2 Objekte), der Microsoft über die von Ihnen wiedergegebenen Stücke informiert. Im Sinne Ihrer Privatsphäre ist es sinnvoll, Alexa und den MediaPlayer von Ad-aware stoppen zu lassen.

Achtung: Wenn auf Ihrem PC eine Personal Firewall läuft, müssen Sie für die Update-Funktion der Datenbank den ausgehenden Datenverkehr auf den Rechner `66.117.38.101` (Zielport `80`) für das Programm Ad-aware freigeben.

Für Profis: Selber suchen

Wer es sich zutraut, kann natürlich auch eigenhändig sein System nach verdächtigen Einträgen durchforsten. Für diesen Zweck ist es hilfreich, wenn man unmittelbar nach der Neuinstallation von MS-Windows und der vorgesehenen Anwendungsprogramme (z.B. MS-Office) eine Kopie der Windows-Registry anfertigt und außerhalb des Systems auf einer CD oder Diskette speichert: Sofern man über die nötige Geduld und Sachkenntnis verfügt, hat man damit jederzeit die Möglichkeit, neue oder modifizierte Registry-Einträge zu finden. Unter Windows 2000 und Windows XP wird die Registry mit dem Programm regedit aufgerufen. Beliebte Verstecke für Trojaner sind vor allem die systemrelevanten Einträge (beginnend mit `HKEY_LOCAL_MACHINE`, `HKEY_CURRENT_CONFIG` und `HKEY_CLASSES_ROOT`) und die benutzerrelevanten Einträge (beginnend mit `HKEY_CURRENT_USER` und `HKEY_USERS`). Eine Liste von Einträgen, die für einen Vergleich mit einer gesicherten Registry besonders empfehlenswert sind, finden Sie unter `http://www.univie.ac.at/ZID/security.html`.

Zusätzlich verbergen sich Trojaner gern in Dateien, die nur beim Systemstart (und auch da oft nur nach der Installation neuer Software) ausgeführt werden – z.B. `c:\windows\winstart.bat` und `c:\windows\wininit.ini`. Einen Überblick über die beim Systemstart ausgeführten Programme erhält man bei Windows XP (als Administrator!) unter *Start – Ausführen*: Tippen Sie hier `msconfig` ein und wählen Sie die Registerkarte *Systemstart*.

Ein modernes Rootkit wird man auf allen diesen Wegen jedoch vergeblich suchen, da es selbstverständlich alle benötigten Registry- und Dateieinträge ausblendet. Bei Rootkits kann es manchmal hilfreich sein, die Festplatte des Betriebssystems über ein Netzwerklaufwerk (Windows-Share) einem anderen Rechner zur Verfügung zu stellen und sich von dort aus umzusehen. Aber Achtung: Schalten Sie zuvor die Miniaturansichten des Systems aus (siehe *Goldene Regeln – Systemkonfiguration – Punkt 2* auf Seite 16) – Sie könnten sonst aus Versehen den Trojaner aktivieren, indem Sie auf ein vermeintliches Dokument-Symbol klicken!

Aron Vrtala ■

Goldene Regeln
für ein intaktes (Windows-)Betriebssystem

In einer Stadt mit bekannt hoher Kriminalität sind Sie sicherlich sehr vorsichtig. Im Internet gilt dies um so mehr: Hier sind Sie mit der ganzen Welt verbunden – vertrauen Sie auf nichts und niemanden! Beherzigen Sie die folgenden Tipps (deren Einhaltung garantiert weniger Mühe macht als einen gekaperten Rechner zurückzuerobern) und halten Sie nicht nur Ihr System, sondern auch sich selbst auf dem Laufenden. Die wichtigsten Querverweise zu aktuellen Sicherheitsinformationen finden Sie unter `http://www.univie.ac.at/ZID/security.html`.

Hygiene

1) Aktivieren Sie für MS-Windows unbedingt die Funktion *Automatische Updates*, die sicherheits- und betriebstechnisch wichtige Komponenten des Systems selbständig aktualisiert (siehe dazu Artikel *Department of Desktop Security: Red Alert bei Windows-Betriebssystemen* auf Seite 18).

2) Installieren Sie einen Virenscanner und einen Trojanerscanner und halten Sie diese immer aktuell (siehe Artikel *McAfee VirusScan: Ihr Goalkeeper im Einsatz gegen virale Offensiven* auf Seite 21).

3) Wiegen Sie sich nicht durch eine vorhandene Institutsfirewall in scheinbarer Sicherheit: Immer wieder gelingt es Hackern, sich durch eine Firewall zu schwindeln; dahinter sind die Angriffsziele oft zahlreich. Installieren Sie daher eine Personal Firewall auf Ihrem Rechner und konfigurieren Sie diese nach Ihren Bedürfnissen: Sperren Sie nicht benötigte (Server-)Dienste, und schränken Sie benötigte Dienste auf den vorgesehenen Benutzerkreis ein.

4) Verwenden Sie immer sichere Passwörter – z.B. die Anfangsbuchstaben eines geheimen Satzes, kombiniert mit Zahlen. Ein solches Passwort lässt sich leicht merken und ist in keinem der elektronischen Wörterbücher zu finden, die von Password Crackern zum Dechiffrieren benutzt werden. Setzen Sie auch einen Bildschirmschoner mit Passwort ein.

5) Denken Sie daran: Der größte Feind eines Rechners sitzt oft vor dessen Tastatur!

Internet

1) Seien Sie beim Bearbeiten von eMail misstrauisch, besonders bei Nachrichten mit Attachments. Sie können davon ausgehen, dass kein einigermaßen seriöses Unternehmen (weder Microsoft noch Hersteller von Virenscannern) Updates oder andere Software per eMail verschickt. Öffnen Sie keine Attachments, die Sie nicht erwartet haben, und bedenken Sie, dass die Mailadresse des Absenders gefälscht sein könnte.

2) Deaktivieren Sie unbedingt die Vorschaufunktion Ihres Mailprogramms – eventuell in einer Nachricht versteckte ausführbare Programme werden sonst automatisch gestartet.

3) Beim Surfen im WWW gilt: Erst nachdenken, dann klicken! So mancher Trojaner kam schon durch ein zu eiliges *OK* ins System.

4) Verwenden Sie nach Möglichkeit verschlüsselte Übertragungsprotokolle: Ersetzen Sie Telnet durch SSH, FTP durch SCP/SFTP und HTTP durch HTTPS. Autorisieren Sie sich im Web nur über HTTPS!

5) Beziehen Sie Free- und Shareware nur von vertrauenswürdigen Quellen (z.B. `http://tucows.univie.ac.at/`) und verzichten Sie auf P2P-Programme – zumindest auf Institutsrechnern und auf Notebooks, die Sie in verschiedenen Netzwerken einsetzen.

Systemkonfiguration

1) Wer stets als Administrator (also mit allen Privilegien) arbeitet, muss bei jedem Mausklick in seinem Webbrowser damit rechnen, dass er durch ein bösartiges ActiveX-Applet die Funktionen seines Rechners gefährdet. Unter Windows 95/98/ME hat man leider keine andere Wahl; unter Windows 2000 und Windows XP kann und soll jedoch ein Einzelnutzer-Betrieb als Administrator vermieden werden.

2) Eine beliebte Aktivierungsmethode für Trojaner sind die standardmäßig leider eingeschalteten Miniaturansichten – das ist jenes Feature, das kleine Abbilder von Grafiken oder Dokumenten erzeugt und diese im Windows Explorer anzeigt. Bei jedem Klick darauf (auch wenn man das Objekt nur zum Löschen markieren möchte!) wird ein allfälliger verborgener Autostart-Trojaner sofort in Gang gesetzt. Unter Windows XP schalten Sie diese Funktion wie folgt aus: Klicken Sie auf ***Arbeitsplatz*** – ***Extras*** – ***Ordneroptionen*** – Registerkarte ***Ansicht*** und entfernen Sie das Häkchen vor der Option *Einfache Ordneransicht in der Ordnerliste des Explorers anzeigen* (siehe Abb. 1). Soll diese Maßnahme die gewünschte Wirkung zeigen, muss zusätzlich die *Details*-Anzeige in der linken Leiste des Windows Explorer geschlossen

sein (d.h. die Pfeile neben *Details* müssen nach unten zeigen; klicken Sie andernfalls auf die Pfeile, um die *Details*-Anzeige zu schließen)!

In der Liste *Ordneroptionen – Ansicht* sollten Sie zusätzlich auch die nächste Option unbedingt deaktivieren (*Erweiterungen bei bekannten Dateitypen ausblenden*; siehe Abb. 1): Manche vermeintliche Grafik wird dann an ihrer zusätzlichen Dateierweiterung als ausführbares Programm erkennbar.

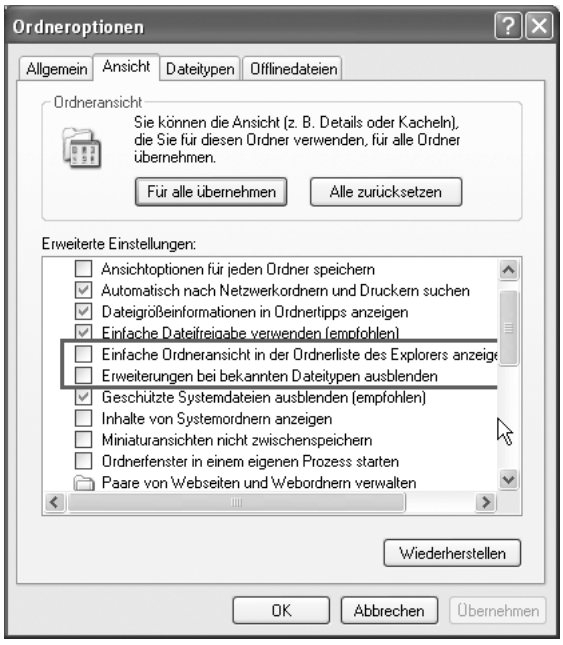

Abb. 1: Windows XP – Fenster *Ordneroptionen*

3) Wenn Sie einen neuen Rechner in Betrieb nehmen, denken Sie über dessen Sicherheitsanforderungen (und die seiner Umgebung!) nach und berücksichtigen Sie das Prinzip der kleinsten benötigten Privilegien. Dies gilt insbesondere auch für Netzwerklaufwerke (Windows-Shares) – öffnen Sie diese nur für Personen, die wirklich auf Ihre Daten zugreifen müssen.

4) Unter Windows NT, 2000, XP und 2003 Server sollten Sie unbedingt NTFS-Dateisysteme einsetzen. Das alte, noch aus DOS-Zeiten stammende FAT- oder FAT32-Dateisystem bietet auf dieser Ebene keinen Schutz vor Fremdzugriff.

5) Erstellen Sie eine Checkliste für die Neuinstallation des Rechners, das hilft in Krisensituationen. Legen Sie diese Checkliste außerhalb des Systems ab!

Weitere nützliche Tipps zum Thema Systemsicherheit finden Sie unter `http://www.univie.ac.at/ZID/security.html` (klicken Sie auf *Vorträge – Vorlesung – Goldene Regeln*).

Aron Vrtala ■

Neue Standardsoftware

Neue Produkte (Stand: 1. 3. 2004)

- Adobe After Effects 6.0 für Win. und Mac
- Adobe GoLive 7 CS für Win. und Mac
- Adobe Illustrator 11 CS für Win. und Mac
- Adobe InDesign 3 CS für Win. und Mac
- Adobe Photoshop 8 CS für Win. und Mac
- Apple MacOS X 10.3
- Corel Designer 10 für Win.
- Corel Painter 8 für Win. und Mac
- Corel Ventura 10 für Win.
- Macromedia Dreamweaver MX 2004 für Win. und Mac
- Macromedia Fireworks MX 2004 für Win. und Mac
- Macromedia Flash MX 2004 für Win. und Mac
- MS-Entourage für Mac
- MS-Frontpage 2003 für Win.
- MS-MapPoint 2004 Euro und US für Win.
- MS-Office 2003 Professional für Win. (Access, Excel, InfoPath, Outlook, PowerPoint, Publisher, Word)
- MS-Office 2003 Standard für Win. (Excel, Outlook, PowerPoint, Word)
- MS-OneNote 2003 für Win.
- MS-Project 2003 Standard und Professional für Win.
- MS-Virtual PC 2004 für Win.
- MS-Visio Standard und Professional 2003 für Win.
- ScanSoft OmniPage Pro 13.0 für Win.
- ScanSoft PaperPort Deluxe 9.0 für Win.
- Sun StarOffice 7 für Win., Linux, Solaris (Lizenz gratis!)
- Symantec pcAnywhere 11.0 für Win.

Updates (Stand: 1. 3. 2004)

- Exceed 9.0 für Win. (bisher 8.0)
- SPSS 12 (bisher 11.5)

Borland-Lizenzen aufgelassen

Wegen geänderter Lizenzbedingungen, äußerst schleppender Lieferungen und sehr schwacher Nachfrage mussten die Softwareprodukte von Borland aus dem Campuslizenz-Programm genommen werden. Bitte kaufen Sie bei Bedarf die Borland-Schulversionen im Fachhandel.

Peter Wienerroither ■

Alle Informationen zur Standardsoftware finden Sie im WWW unter `http://www.univie.ac.at/zid-swd/`.

Achtung: Änderungen bei Software-Bestellungen für die Med-Uni (siehe Seite 2)!

Department of Desktop Security: **RED ALERT BEI WINDOWS-BETRIEBSSYSTEMEN**

Hacker, Viren, Würmer, trojanische Pferde – das Spektrum möglicher Bedrohungsszenarien ist in der global vernetzten IT-Welt während der letzten Dekade kräftig angewachsen. Um den vielfältigen Herausforderungen zu begegnen und einigermaßen befriedigende Sicherheitskonstruktionen für Rechner und Netzwerke zu schaffen, bemühen sich IT-Security-Experten, gefährdete Bereiche zu analysieren und mögliche Angriffspunkte aufzuspüren. Auch gängige Betriebssysteme weisen – nicht zuletzt aufgrund immer kürzerer Entwicklungszyklen – mehr oder minder gravierende Sicherheitslecks auf. Verursacher sind hier Programmierfehler, welche allzu oft erst in der allgemeinen Anwendungsphase erkannt werden. Möchte der Benutzer diese im Nachhinein beheben, ist er in der Regel davon abhängig, ob und wie bald der Hersteller entsprechende Programmkorrekturen – in Form von so genannten *Patches* („Flicken") – bereitstellt.

In letzter Zeit hat insbesondere das erfolgsverwöhnte Unternehmen Microsoft einen nicht abreißen wollenden Strom an Negativschlagzeilen in der einschlägigen Fachpresse erzeugt: Immer wieder wird von neuen, als „kritisch" eingestuften Sicherheitslücken in Windows-Betriebssystemen berichtet, die unverzüglich durch die Installation der entsprechenden Sicherheits-Updates behoben werden sollten. Wird dies verabsäumt und lernen potentielle Angreifer erst derlei Schwachstellen zu nutzen, stellen sie eine durchaus ernst zu nehmende Gefahr für die Sicherheit ungeschützt betriebener Rechner dar.

Von Seiten Microsofts wird in diesem Zusammenhang gerne darauf hingewiesen, dass es in vielen Fällen bereits effiziente Lösungen gäbe, die den Kunden auch kostenlos zur Verfügung gestellt würden. Nicht das mangelnde Vorhandensein eines Schutzes stelle das eigentliche Problem dar, sondern vielmehr die mangelnde Bereitschaft der Anwender, diesen – in Form der erforderlichen Security Patches – rechtzeitig zu installieren.

Aus Sicht der BenutzerInnen präsentiert sich dies freilich aus einer anderen Perspektive. Das hierfür notwendige regelmäßige „Einspielen" (d.h. das Herunterladen und Installieren) von neuen Patches wird auf Dauer als eine lästige Angelegenheit wahrgenommen. Zudem stößt es vielen sauer auf, durch derartige „Nachbesserungsarbeiten" noch stärker in ein Abhängigkeitsverhältnis zu dem Softwaregiganten zu geraten.

Allen Bedenken zum Trotz: Solange der Erwerb eines hochprozentig sicheren Betriebssystems der Kategorie „visionäres Wunschdenken" zuzuordnen ist, lässt sich bei nüchterner Abwägung der möglichen Risiken nur eine Empfehlung geben: *Take What You Can Get*. Oder besser:

Flicken was das Zeug hält

Um den Aufwand des regelmäßigen Updatens zu minimieren und sicherzustellen, dass zumindest die wichtigsten Security Patches (von Microsoft als *Hotfixes* bezeichnet) rechtzeitig installiert werden, empfiehlt es sich, das lokale Windows-Update-Dienstprogramm *Automatische Updates* zu nutzen. Es wird von den aktuelleren Windows-Versionen Windows XP, Windows 2000 mit Service Pack 3 (SP3) oder höher, Windows ME sowie Windows Server 2003 unterstützt.[1)]

Im Gegensatz zum manuellen Updaten, dem zunächst eine mehr oder minder lange Orientierungs- und Auswahlphase auf den Webseiten von Microsoft vorausgeht, ist das Funktionsprinzip von *Automatische Updates* effizient und benutzerfreundlich: Sobald Sie mit dem Internet verbunden sind, begibt sich *Automatische Updates* auf die Suche nach neuen wichtigen Aktualisierungen für Ihr System. Wird es dabei fündig, orientiert sich seine weitere Vorgehensweise an den von Ihnen gewählten Einstellungen: Entweder informiert es Sie, dass neue, wichtige Updates verfügbar sind und fragt nach, ob diese jetzt heruntergeladen werden sollen, oder es lädt die Patches automatisch im Hintergrund herunter. Sie können währenddessen ungestört an Ihrem Rechner weiterarbeiten.

Nach Beendigung des Downloads erhalten Sie eine Verständigung, dass jetzt neue Updates installiert werden können. Von hier aus trennen Sie nur mehr ein paar Mausklicks und gegebenenfalls ein Neustart Ihres Rechners von der erfolgreichen Behebung einer Reihe von Sicherheitslecks in Ihrem Windows-Betriebssystem.

Das Dienstprogramm *Automatische Updates* unter Windows XP

Eine detaillierte Beschreibung, wie Sie unter Windows XP *Automatische Updates* einrichten und Security Patches korrekt installieren, entnehmen Sie bitte der folgenden Anleitung (wie Sie die Konfiguration unter Windows 2000 vornehmen, können Sie unter `http://www.ap.univie.ac.at/security/minimum_win2k.html` nachlesen). Beachten Sie: Zum Ändern der Einstellungen unter *Automatische*

1) Für die älteren Betriebssysteme Windows 95, Windows 98 und Windows NT stehen Systemupdates von Microsoft nicht mehr bzw. nur mehr in seltenen Ausnahmefällen zur Verfügung. Da die Sicherheit des Systems demnach nicht mehr garantiert werden kann, ist es hier angeraten – sofern irgend möglich – ein Systemupgrade auf Windows XP durchzuführen.

2) Falls Sie in der Systemsteuerung die „klassische Ansicht" voreingestellt haben, überspringen Sie den Punkt *Leistung und Wartung*.

Updates müssen Sie als Administrator oder als Mitglied der Gruppe Administratoren angemeldet sein.

Wählen Sie ***Start – (Einstellungen –) Systemsteuerung – Leistung und Wartung***[2] ***– System***. Mit einem Doppelklick auf *System* öffnen Sie das Fenster *Systemeigenschaften*. Wechseln Sie hier mit einem Klick zur Registerkarte ***Automatische Updates*** (siehe Abb. 1).

Befindet sich ein Häkchen in dem Kästchen neben dem Text ***Den Computer auf dem neuesten Stand halten (Durch Aktivieren dieser Einstellung kann Windows Update-Software automatisch vor dem Anwenden anderer Updates aktualisiert werden.)***, so ist dieser Dienst aktiviert. Sollte dies nicht der Fall sein, aktivieren Sie ihn, indem Sie auf das Kästchen klicken.

Ein Stück weiter unten auf der Registerkarte können Sie unter *Einstellungen* festlegen, welche Vorgangsweise Sie für den automatischen Download und die anschließende Installation wünschen (vgl. Abb. 1). Bei Auswahl der Option 1 werden Sie zweimal benachrichtigt – vor dem Download der Updates und vor deren Installation. Option 2 (üblicherweise voreingestellt) informiert Sie erst, sobald Updates zur Installation bereitstehen. Option 3 (nur Windows XP Professional) ermöglicht es Ihnen, die automatisch heruntergeladenen Updates anhand eines Zeitplanes zu installieren.

Stellen Sie die Konfiguration wie folgt ein: ***Updates automatisch downloaden und über installierbare Updates benachrichtigen*** – oder konfigurieren Sie ein automatisches Downloaden von Updates und lassen Sie das System diese *laut angegebenen Zeitplan installieren*. Wenn Ihr System ohnehin in der Nacht durchläuft, wäre dies die optimale Lösung. Wählen Sie dann *Täglich* und lassen Sie die Installation z.B. um *02:00* Uhr in der Nacht durchführen.

Für den Fall des händischen Startens der Installation müssen Sie sich als Administrator anmelden. Sobald neue Softwarekorrekturen verfügbar sind, erscheint rechts unten in Ihrer Taskleiste eine Sprechblase mit dem Text *Neue Updates können jetzt installiert werden* (siehe Abb. 2). Diese Information erlischt nach kurzer Zeit. Sie können später das Vorhandensein von Updates anhand des (in Abb. 3 ganz links sichtbaren) kleinen Windows-Symbols im Infobereich Ihrer Taskleiste erkennen.

Wenn Sie die Installation starten wollen, doppelklicken Sie auf das Symbol. Es erscheint das Fenster *Automatische Updates – Installationsbereit* (siehe Abb. 4). Unter ***Details*** können Sie eine Liste der empfohlenen Updates einsehen.

Bestätigen Sie dann mit ***Installieren***, um die Installation auszuführen. Für einige Updates ist es möglicherweise erforderlich, Ihren Computer erneut zu starten, um die Installation abzuschließen. Führen Sie in diesem Fall unbedingt einen Neustart durch, da sonst die Korrekturen nicht wirksam werden können!

Ein Tipp zum Abschluss: Sollten Sie sich entschließen, ein bestimmtes heruntergeladenes Update nicht zu installieren,

Abb. 2:
Infobereich von Windows XP – Benachrichtigung über neue Updates

Abb. 3:
Das Symbol ganz links im Infobereich der Windows-Taskleiste zeigt an, dass neue Updates installationsbereit sind.

Abb. 1: Fenster *Systemeigenschaften – Automatische Updates*

Abb. 4: Fenster *Automatische Updates – Installationsbereit*

löscht Windows die zugehörigen Dateien von Ihrem Computer. Falls Sie Ihre Meinung später ändern, ist es relativ einfach möglich, diese Updates erneut herunterzuladen: Unter ***Start – (Einstellungen –) Systemsteuerung – Leistung und Wartung***[2] – ***System*** – Registerkarte ***Automatische Updates*** finden Sie rechts unten die Schaltfläche ***Abgelehnte Updates***. Klicken Sie darauf, um einen wiederholten Download zu initiieren. Wenn die zuvor abgelehnten Updates weiterhin für den Computer geeignet sind, werden sie angezeigt, sobald Sie das System das nächste Mal über verfügbare Updates informiert.

Michaela Bociurko ■

SICHERHEIT VON ANFANG AN

Windows XP mit Firewall-Schutz installieren

Antivirenprogramme und Personal Firewalls sind eine feine Sache – sobald sie einsatzbereit sind. Wenn man aber einen neuen Rechner erstmals an das Netzwerk anschließt, um einen Virenscanner bzw. eine Firewall herunterzuladen und zu installieren, ist der Rechner bis zur Inbetriebnahme dieser Programme ungeschützt. Falls er sich in einem verseuchten Netz befindet, ist er mit hoher Wahrscheinlichkeit dann auch bereits mit Viren und/oder Trojanern infiziert. Bei Windows XP lässt sich diese gefährliche Lücke mit Hilfe der integrierten Firewall (die standardmäßig jedoch deaktiviert ist) schließen.

Hinweis: Eine gesicherte Installation von Windows 2000 verläuft fast genau so wie hier für Windows XP beschrieben – nur bei Punkt 3 sollte eine Personal Firewall von einer CD aus installiert und mit einem „allgemeinen Eintrittsverbot" konfiguriert werden. Nach der Installation der Windows-Updates und des Virenscanners kann man die Konfiguration der Firewall bei Bedarf wieder lockern.

Die folgende Anleitung geht von einem Gerät mit bereits installierter Netzwerkkarte und noch zu installierendem Betriebssystem aus; das Netzwerkkabel ist **nicht** angesteckt. Da sich diverse Schädlinge auch sehr gerne – und in unserem Szenario vom Benutzer leider völlig unbemerkt – über Funk-LANs ausbreiten, muss ein integrierter WLAN-Adapter gegebenenfalls zuerst im BIOS des Rechners deaktiviert werden. Vorsicht: Änderungen an den BIOS-Einstellungen sind eine heikle Angelegenheit und sollten nur von erfahrenen BenutzerInnen mit guten Fachkenntnissen vorgenommen werden!

1. Installieren Sie Windows XP von der CD. Die folgenden Schritte müssen Sie als Administrator durchführen.

2. Konfigurieren Sie die Netzwerkkarte über ***Start – (Einstellungen –) Systemsteuerung – Netzwerkverbindungen*** – Klick mit der **rechten** Maustaste auf ***LAN-Verbindung*** (bei mehreren Netzwerkkarten sind eventuell mehrere LAN-Verbindungen vorhanden) – ***Eigenschaften***. Im Fenster *Eigenschaften von LAN-Verbindung* wählen Sie auf der Registerkarte ***Allgemein*** den Punkt ***Internetprotokoll (TCP/IP)*** und geben dort die erforderlichen Einstellungen an.

3. Klicken Sie nun im Fenster *Eigenschaften von LAN-Verbindung* auf die Registerkarte ***Erweitert*** und aktivieren Sie hier die integrierte Firewall von Windows XP (das Kästchen muss angehakt sein; siehe Abb. 1). Schließen Sie das Fenster durch Klick auf ***OK***.

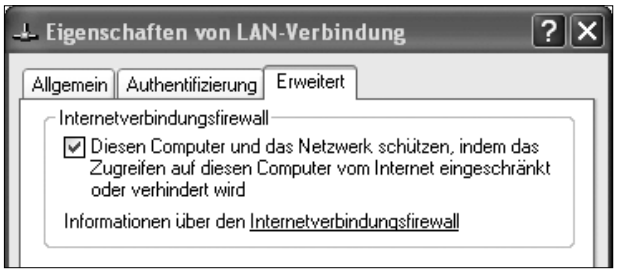

Abb. 1: Fenster *Eigenschaften von LAN-Verbindung* – Internetverbindungsfirewall ist aktiviert

4. Stecken Sie das Netzwerkkabel an.

5. Unmittelbar danach müssen Sie über ***Start – (Einstellungen –) Systemsteuerung – System*** – Registerkarte ***Automatische Updates*** die aktuellen Windows-Updates einspielen (siehe dazu auch Artikel *Department of Desktop Security: Red Alert bei Windows-Betriebssystemen* auf Seite 18).

6. Anschließend installieren Sie den gewünschten Virenscanner und führen sofort ein Update der Virendatenbank durch (siehe dazu auch den Artikel *McAfee VirusScan – Ihr Goalkeeper im Einsatz gegen virale Offensiven* auf Seite 21).

7. Nun können Sie gegebenenfalls weitere Netzwerkadapter (z.B. WLAN) aktivieren. Schützen Sie diese ebenfalls – wie oben beschrieben – über die XP-Firewall.

8. Die weitere Installation verläuft wie gewohnt: Benutzer einrichten, Anwendungssoftware installieren usw. Wenn gewünscht, können Sie jetzt auch eine andere Personal Firewall installieren und einrichten. Die XP-Firewall sollten Sie in diesem Fall nach der Installation der neuen Firewall wieder deaktivieren.

Aron Vrtala ■

McAfee VirusScan

Ihr Goalkeeper im Einsatz gegen virale Offensiven

Die gegnerische Offensive prescht vor, doch kein Verteidiger, kein Schlussmann in Sicht! Der Angreifer kickt in Richtung des unbewachten Tores – die Menge brüllt: TOR! TOR! TOR!

Wäre dieses Szenario wirklich denkbar? Jene, welche dem runden Leder zugetan sind, schütteln jetzt wohl nur verständnislos den Kopf. Dennoch verhalten sich einige EDV-AnwenderInnen durchaus vergleichbar, wenn sie auf den Einsatz effektiver Antivirensoftware verzichten: Ihr Rechner verbleibt ungeschützt gegen jegliche virale Offensive. Was im Sport schlimmstenfalls eine Niederlage herbeiführt, kann jedoch für Ihren Rechner fatale Auswirkungen haben. Hat ein Virus erst einmal „erfolgreich" zugeschlagen, sind Arbeitsaufwand, Datenverlust und – nicht zuletzt – meist beträchtliche Kosten die unweigerlichen Folgen. Für infizierte Notebooks sind noch weitreichendere Konsequenzen denkbar, da diese Geräte aufgrund ihrer Mobilität ein deutlich höheres Risikopotential darstellen. Infektionen können hiermit von einem Netzwerk in ein anderes übertragen werden und in der Folge beispielsweise alle Rechner eines Betriebs verseuchen.

Um Sie vor derartigen Geschehnissen zu bewahren, haben wir Ihnen den folgenden kleinen Crashkurs zusammengestellt, der Ihnen – als frisch gebackenem Manager, Trainer und Präsidenten in einer Person – Schritt für Schritt helfen soll, eine schlagkräftige Verteidigung für Ihren Rechner aufzubauen.

Punkt 1: Kaderauswahl

Selektion einer geeigneten Antivirensoftware

Der Entschluss, eine effektive Abwehr für Ihren Rechner aufzustellen, ist gefällt. Nun drängt sich die Frage auf, wen Sie mit der anspruchsvollen Position des Torwächters betrauen möchten.

Grundsätzlich wird am Softwaremarkt eine breite Palette von Antivirenprogrammen angeboten. Da die Uni Wien für den Virenscanner von McAfee eine Campuslizenz besitzt, steht dieser allen Uni-MitarbeiterInnen kostenlos zur Verfügung. Voraussetzung für den Download vom SWD-Server der Universität Wien ist in jedem Fall eine gültige Mailbox-UserID.

Derzeit sind zwei Versionen in Gebrauch: McAfee VirusScan Enterprise 7.x und die Version 4.5.x.

- McAfee VirusScan Enterprise 7.x ist die aktuellere Version und weist einige neue, durchaus brauchbare Features auf. Betriebssystemvoraussetzung ist für diese Version Windows NT 4.0 (SP6 oder höher), Windows 2000 Professional oder Windows XP.

- Sollten Sie einen Rechner mit Windows 95, 98 bzw. ME-Betriebssystem verwenden, installieren Sie bitte die Version 4.5.x.

Beachten Sie, dass sich die detaillierten Anleitungen in diesem Artikel auf die neuere Version Enterprise 7.x beziehen. Die beiden Versionen sind in Prinzip und Funktionsumfang zwar weitgehend ident, jedoch können diverse Darstellungen bei der Version 4.5.x etwas abweichen.

Download und Installation

1. Rufen Sie in Ihrem Browser den URL **`http://swd.univie.ac.at/`** auf, klicken Sie auf ***Weiter*** und identifizieren Sie sich anhand Ihrer Mailbox-UserID und Ihres Mailbox-Passworts.

2. Sie erhalten eine Liste aller für Sie verfügbaren Softwareprodukte. Klicken Sie ganz oben in der Liste auf ***Gratissoftware*** und auf der folgenden Seite auf ***McAfee Virenscanner***.

3. Sie finden dort einen Link ***zum Server von NAI*** (Network Associates International, der Herstellerfirma von McAfee) und genaue Informationen für den Download des Virenscanners.

4. Nachdem die komprimierte `.zip`-Datei auf Ihren Rechner übertragen wurde, muss sie entpackt werden. Falls Sie dafür keine geeignete Software installiert haben, müssen Sie noch unter ***Gratissoftware – WinZip*** die Datei ***winzip81.exe*** (für Windows 95/98/ME/NT/2000/XP, Englisch) auf Ihren Rechner übertragen. Führen Sie die `.exe`-Datei anschließend durch einen Doppelklick aus, wählen Sie ein Verzeichnis zum Entpacken und installieren Sie dort das Programm durch einen Doppelklick auf die Datei ***setup.exe***.

5. Entpacken Sie nun die `.zip`-Datei durch einen Doppelklick und installieren Sie das Antivirenprogramm durch einen Doppelklick auf ***setup.exe***. Dabei können Sie getrost die Standardvorgaben verwenden; die Installation selbst geht automatisch vor sich.

6. Da die Uni Wien nur über eine begrenzte Anzahl von Lizenzen für McAfee bzw. WinZip verfügt, bitten wir Sie, die Verwendung der Programme per eMail bekannt zu geben (*To*: `peter.wienerroither@univie.ac.at`; *Subject*: McAfee-Registrierung bzw. WinZip-Registrierung; *Inhalt*: Name, Institut, Tel., Anzahl der Lizenzen).

Punkt 2: Training

Halten Sie Ihre Defensive up-to-date

Der Gegner schläft nicht. Täglich ersinnt er neue Taktiken, Ihren Torhüter auszuspielen. Verhindern können Sie dies nur, indem Sie ihn für die jeweils aktuellen Herausforderungen fit erhalten. Zu diesem Zweck sind Updates vorgesehen. Sie sind das unbedingt notwendige, regelmäßige „Training" Ihres „Spielers": Der Virenscanner ist mit einer internen Virendatenbank ausgestattet, in welcher Signaturen von bereits bekannten Viren enthalten sind. Werden während eines Scanprozesses verdächtige Codes entdeckt, vergleicht der Virenscanner seine Untersuchungsergebnisse mit dem Inhalt seiner Datenbank und kann so mutmaßliche Viren einwandfrei identifizieren. Da täglich neue Viren auftauchen, muss dieser Erkenntnisstand regelmäßig aufgefrischt werden. Ohne die aktualisierten Dateien kann die Software neue Viren unter Umständen nicht erkennen oder nicht entsprechend auf diese reagieren. Die Aktualität der Virendatenbank ist demnach entscheidend für die Effektivität der Erkennung.

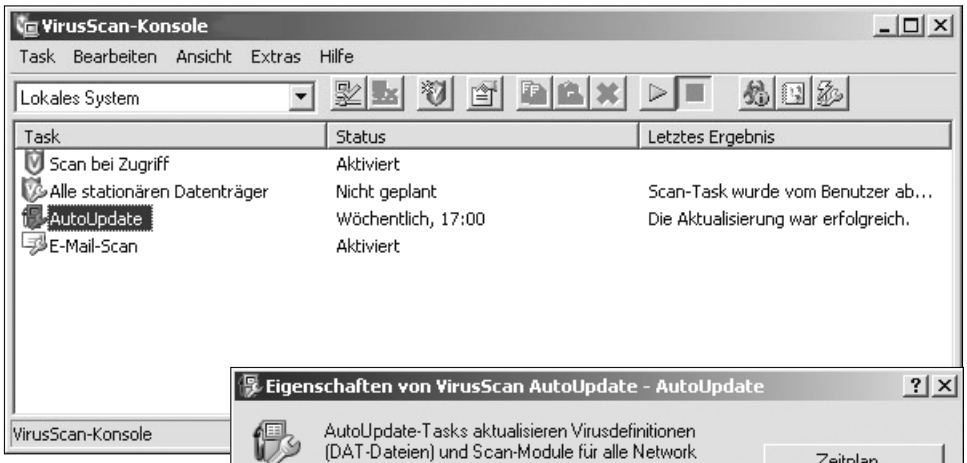

Abb. 1: Die VirusScan-Konsole von McAfee

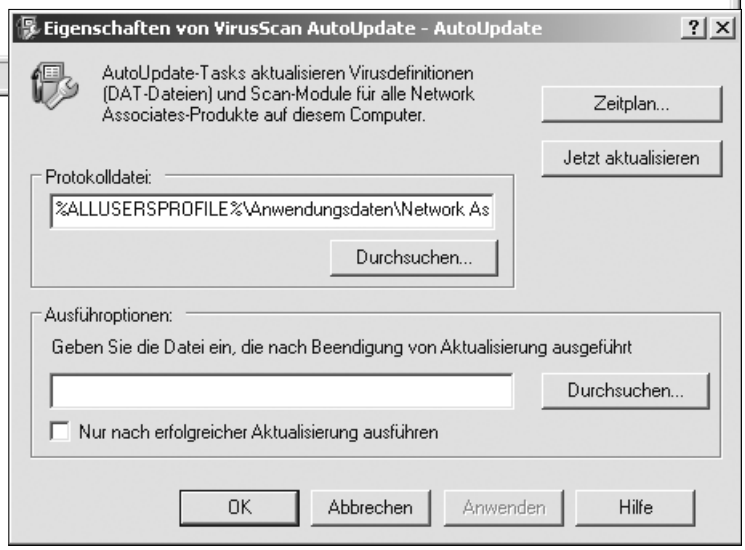

Abb. 2: Fenster *Eigenschaften von VirusScan AutoUpdate*

AutoUpdate

McAfee VirusScan bietet eine AutoUpdate-Funktion, anhand derer das Updaten ohne großen Aufwand für den Benutzer und in garantierter Regelmäßigkeit durchgeführt werden kann. Bei diesem automatisierten Prozess greift das Programm auf eine Download-Seite (ein so genanntes *Repository*) zu und lädt die entsprechenden Aktualisierungen von dort herunter. Standardmäßig bezieht Ihr VirusScan seine Aktualisierungen vom FTP- bzw. HTTP-Repository des Herstellers Network Associates International. Die hierfür notwendige Konfiguration wird nach Abschluss der Installation automatisch vorgenommen. Sie müssen sich also nicht weiter mit der Frage beschäftigen, woher Sie Ihre Updates beziehen. Viel wichtiger ist die Überlegung, wann Sie diese abrufen.

Mithilfe der AutoUpdate-Funktion kann das Updaten sowohl manuell per Direktanfrage als auch anhand eines Zeitplanes durchgeführt werden. Nutzen Sie die äußerst praktische Möglichkeit des Updatens via Zeitplan. Dieser ermöglicht es Ihnen, die verschiedenen Parameter nach Ihren persönlichen Präferenzen festzulegen. Die Aktualisierungen werden dann automatisch anhand dieser Zeitsteuerung vorgenommen. Die Enterprise-Version von McAfee bietet einen vordefinierten Aktualisierungs-Task, der jeden Freitag um 17:00 Uhr durchgeführt wird (mit einstündiger Zufallsfunktion). Es ist ratsam, diesen standardmäßigen Aktualisierungs-Task neu zu konfigurieren. Nehmen Sie sich kurz Zeit, die Einstellungen auf Ihre persönlichen Bedürfnisse abzustimmen. Die entsprechenden Änderungen sind einfach und schnell durchgeführt:

Wählen Sie ***Start – Programme – Network Associates – VirusScan-Konsole*** (siehe Abb. 1). Doppelklicken Sie auf ***AutoUpdate.*** Das Fenster *Eigenschaften von VirusScan AutoUpdate*[1)] öffnet sich (siehe Abb. 2). Durch Anklicken der Schaltfläche ***Zeitplan*** gelangen Sie in das Fenster *Zeitplaneinstellungen.* Da der Task hier bereits aktiviert ist, wechseln Sie gleich mit einem Klick auf die Registerkarte ***Zeitplan*** (siehe Abb. 3).

Unter *Geplanter Task* finden Sie die standardmäßige Konfiguration vor (*Wöchentlich*). Ändern Sie diese, indem Sie den Listenpfeil rechts neben dem Kästchen anklicken. Die nun sichtbare Liste präsentiert Ihnen eine Reihe von Optionen:

- Für BenutzerInnen mit Wählleitungszugang ist es naheliegend, das AutoUpdate ***Beim Einwählen*** durchführen zu lassen.

- Rechner, die via Breitband mit dem Internet verbunden bzw. in LAN-Netze eingebunden sind und beinahe täg-

1) Hier können Sie auch manuell per Direktanfrage neue Updates abrufen, indem Sie auf ***Jetzt aktualisieren*** klicken. Ein AutoUpdate wird dann umgehend durchgeführt.

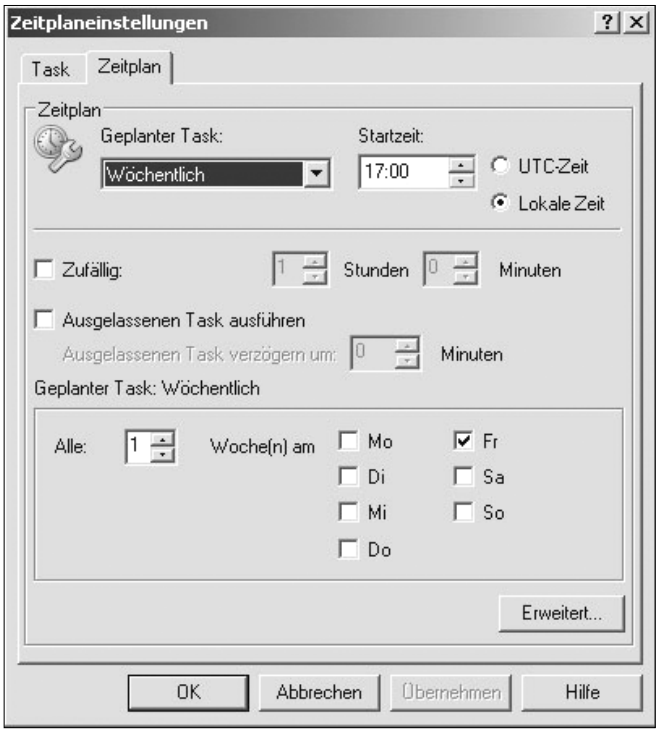

Abb. 3: Fenster *Zeitplaneinstellungen*, Registerkarte *Zeitplan*

lich ein- und ausgeschaltet werden („Werktagsrechner"), sollten zumindest ***Bei Systemstart*** aktualisiert werden.

- Bei Geräten, die auch in der Nacht nicht ausgeschaltet werden, ist wenigstens ein Update ***Täglich*** zu einer von Ihnen gewählten Uhrzeit (z.B. *07:00*) empfehlenswert.

Wählen Sie die für Sie passende Einstellung und schließen Sie den Task ab, indem Sie auf ***Übernehmen*** klicken und mit ***OK*** bestätigen.

Punkt 3: Techniken

Automatisches und manuelles Scannen

Die ersten beiden Punkte haben Sie souverän absolviert. Ihr „Goalie" ist in Ihr Team integriert und erhält ein regelmäßiges, perfekt auf Ihren Spielplan abgestimmtes Fitnessprogramm. Vor einem Einsatz auf dem Feld sollten Sie sich allerdings unbedingt mit den Fertigkeiten Ihres Neuerwerbs vertraut machen. Es gilt, zumindest einige wichtige Techniken Ihres Virenscanners zu kennen und zu wissen, wie Sie diese effektiv anwenden können.

Mit McAfee VirusScan können zwei Arten von Scanvorgängen ausgeführt werden:

- Automatisches Scannen,
- Scannen in regelmäßigen Abständen, bei Auswahl oder zu festgelegten Zeiten.

Abb. 4: Infobereich von Windows XP – Scannen bei Zugriff ist deaktiviert

Scannen bei Zugriff

Die automatische Virenprüfung wird als *Scannen bei Zugriff* bezeichnet. Diese Funktion scannt in allen Dateien, die Sie öffnen, kopieren, speichern oder anderweitig bearbeiten sowie in allen Dateien, die Sie von Disketten oder Netzwerklaufwerken lesen oder auf diese schreiben. Sie bietet somit ständigen Schutz vor Viren, welche in diesen Quellen lauern.

Scannen bei Zugriff ist gewöhnlich nach erfolgreicher Installation aktiviert. Überprüfen Sie dies, indem Sie nach dem VShield-Symbol im Windows-Infobereich (rechts unten) Ausschau halten. Sollte wider Erwarten *Scannen bei Zugriff* deaktiviert sein, erkennen Sie dies an einem kleinen durchgestrichenen roten Kreis innerhalb des VShield (siehe Abb. 4). In diesem Fall doppelklicken Sie darauf und wählen Sie dann ***Aktivieren***. ***Schließen*** Sie das Fenster. Ihr Virenscanner ist nun stets wachsam.

Detailliertere Optionen können Sie ebenso mit einem Doppelklick auf das VShield aufrufen: Unter ***Eigenschaften*** ist es möglich, umfangreiche Konfigurationen für den Scanvorgang bei Zugriff vorzunehmen. So kann hier speziell definiert werden, welche Bereiche bei Anwendung dieses Tasks mit einbezogen werden sollen, welchen Ordner man für die Quarantäne-Funktion heranziehen möchte und wie lange der Scanvorgang für einzelne Bereiche dauern darf. Darüber hinaus lassen sich Aktionen wie das Versenden von Benutzernachrichten über Virusaktivitäten (*Wer bekommt welche Nachricht?*) oder das Erstellen von Protokollen (*Soll protokolliert werden, wenn ja wo und wie viel?*) genauer spezifizieren.

Unter *Alle Vorgänge* können Sie außerdem *Unterschiedliche Einstellungen für Vorgänge mit niedrigem oder hohem Risiko verwenden*. Dieses Feature mag zum Teil nützlich sein für den erfahrenen Benutzer, der Wert darauf legt, jede Einstellung individuell festzulegen. Für die herkömmliche Anwendung empfiehlt es sich jedoch, die Standardeinstellung des Herstellers (*Einstellungen auf diesen Registerkarten für alle Vorgänge verwenden*) zu belassen.

Scannen auf Anforderung

Neben dem permanenten Scannen sollten Sie auch unbedingt regelmäßig die komplette Festplatte auf Viren durchsuchen. Vielleicht haben Sie ja vor einigen Wochen schon ein Virus auf der Festplatte gespeichert, das der Virenscanner damals noch nicht kannte und das bei Ihnen bis dato noch nicht aktiviert wurde. Mit dem *Scannen auf Anforderung* verfügen Sie über eine Methode, mit der Sie alle Teile des Computers zu für Sie günstigen Zeiten oder in regelmäßigen Abständen auf Viren scannen können. Verwenden Sie den Anforderungsscan als Ergänzung zum kontinuierlichen Schutz durch den Zugriffsscanner. Der integrierte Zeitplan hilft Ihnen dabei, die regelmäßigen Scanvorgänge so festzulegen, dass Ihre Arbeitsabläufe nicht eingeschränkt werden. Wählen Sie vorzugsweise eine Zeit-

spanne aus, in der Sie nicht am Gerät arbeiten (beispielsweise um die Mittagszeit oder nachts), da der Vorgang in den meisten Fällen die Systemleistung Ihres PCs beeinträchtigt.

Die VirusScan-Konsole enthält einen Standard-Task für das *Scannen auf Anforderung* mit dem Namen *Alle stationären Datenträger*. Sie können diesen Task umbenennen und /oder eine unbegrenzte Anzahl von (neuen) Anforderungstasks anlegen. Einen neuen Anforderungsscan erstellen Sie, indem Sie aus dem Menü ***Task*** die Option ***Neuer Scan-Task*** auswählen. In der Task-Liste der VirusScan-Konsole wird jetzt ein ***Neuer Scan*** angezeigt. Doppelklicken Sie darauf um die Konfiguration des Anforderungsscans vorzunehmen. Im Fenster *VirusScan – Scannen auf Anforderung – Eigenschaften – Neuer Scan* können Sie nun festlegen, welche Elemente zu welchem Zeitpunkt gescannt werden sollen, welche Reaktion erfolgt, wenn Viren gefunden werden, und wie Sie in einem solchen Fall benachrichtigt werden wollen.

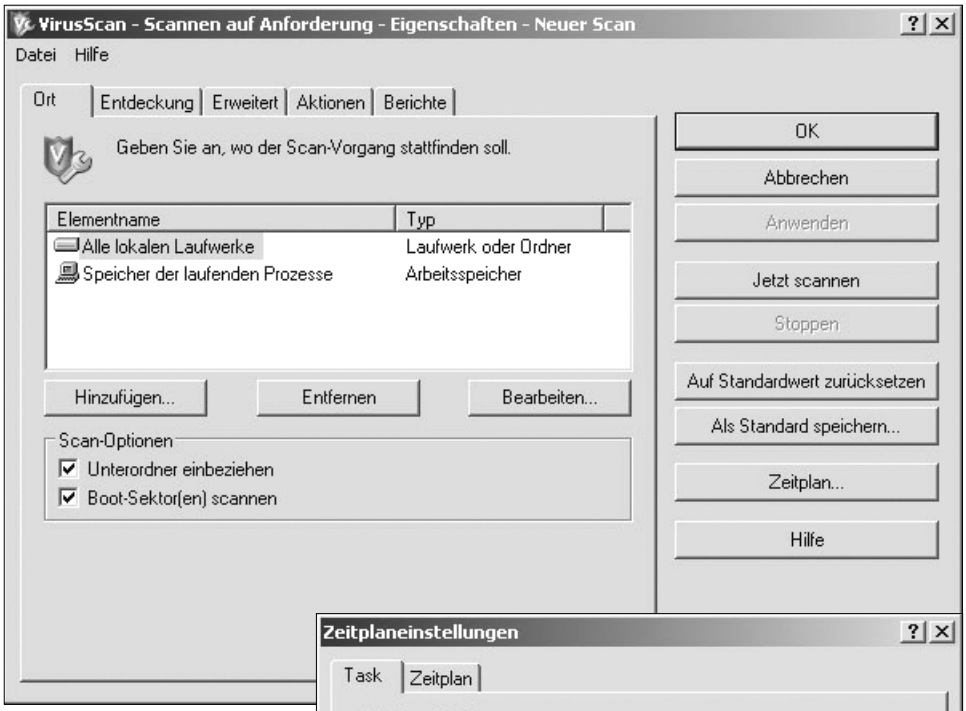

Abb. 5: Fenster *VirusScan – Scannen auf Anforderung – Eigenschaften – Neuer Scan* – Registerkarte *Ort*

Jene Bereiche, die gescannt werden sollen, werden auf der Registerkarte *Ort* definiert (siehe Abb. 5). Standardmäßig werden folgende Einstellungen verwendet: Auf allen lokalen Laufwerken, im Speicher der laufenden Prozesse, in den Unterordnern sowie in den Bootsektoren. Diese voreingestellte Auswahl hat Sinn, kann aber unter Umständen sehr lange dauern. Ändern Sie sie nur in Ausnahmefällen, beispielsweise wenn für den Scanvorgang lediglich ein sehr beschränkter Zeitrahmen zur Verfügung steht.

Auf der Registerkarte *Entdeckung* werden die Elemente definiert, die überprüft werden sollen. Auch hier ist die Voreinstellung *Alle Dateien* als sinnvoll zu erachten und zu belassen. Unter *Erweitert* können Sie – nomen est omen – erweiterte Optionen festlegen. Standardmäßig ist lediglich die *Heuristik* aktiviert. Mit diesem Begriff wird ein Suchverfahren bezeichnet, bei dem Programme nach „verdächtigen" Befehlsfolgen durchsucht werden, also nach (noch) nicht bekannten Virencodes. Die Effizienz dieser Methode ist derzeit jedoch laut Sicherheitsexperten eher minimal. Zudem ist sie äußerst fehleranfällig, was sich in zahlreichen *False Positives* bemerkbar macht. Sie können diese Funktion also unbesorgt deaktivieren.

Unter *Aktionen* wird festgelegt, wie der Virenscanner vorgehen soll, wenn er ein Virus gefunden hat. Generell wird empfohlen, im Zweifelsfall immer die Aktion *Säubern* zu

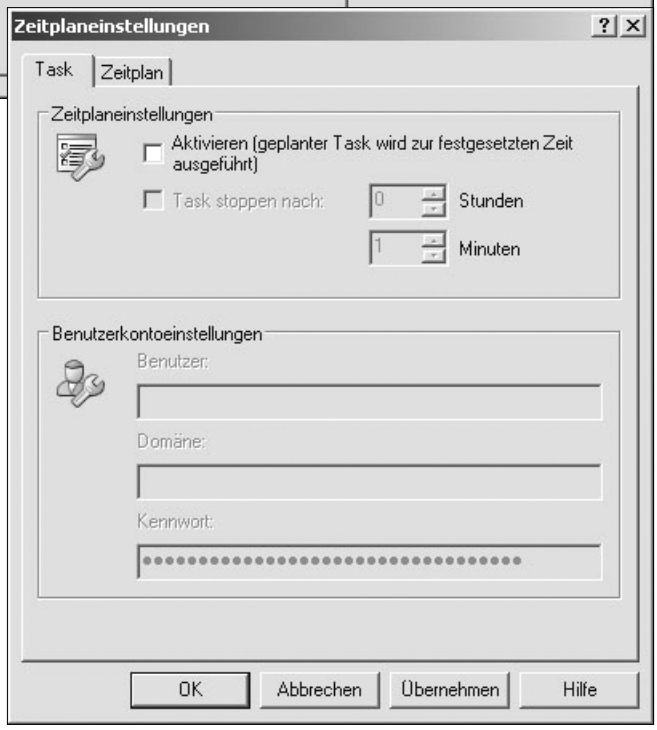

Abb. 6: Fenster *Zeitplaneinstellungen*, Registerkarte *Task*

wählen. Dies ist auch standardmäßig in VirusScan Enterprise vorgegeben. Wenn das Säubern der Datei fehlschlägt, verschiebt Ihr Scanner die Datei automatisch in den Ordner *Quarantäne*, der bereits bei der Installation des Programms angelegt wurde.

Auf der letzten Registerkarte *Berichte* können Sie schließlich diverse Einstellungen zu den Protokolleinträgen vornehmen, die der Virenscanner zu Ihrer Information erstellt. Die Optionen ermöglichen es Ihnen, den Ablageort selbst zu bestimmen (*Durchsuchen*) bzw. die *Größe* der Protokolldatei zu *begrenzen* (1 bis 999 MB). Wenn Sie keine Protokollierung wünschen, deaktivieren Sie einfach die Option *In Datei protokollieren*.

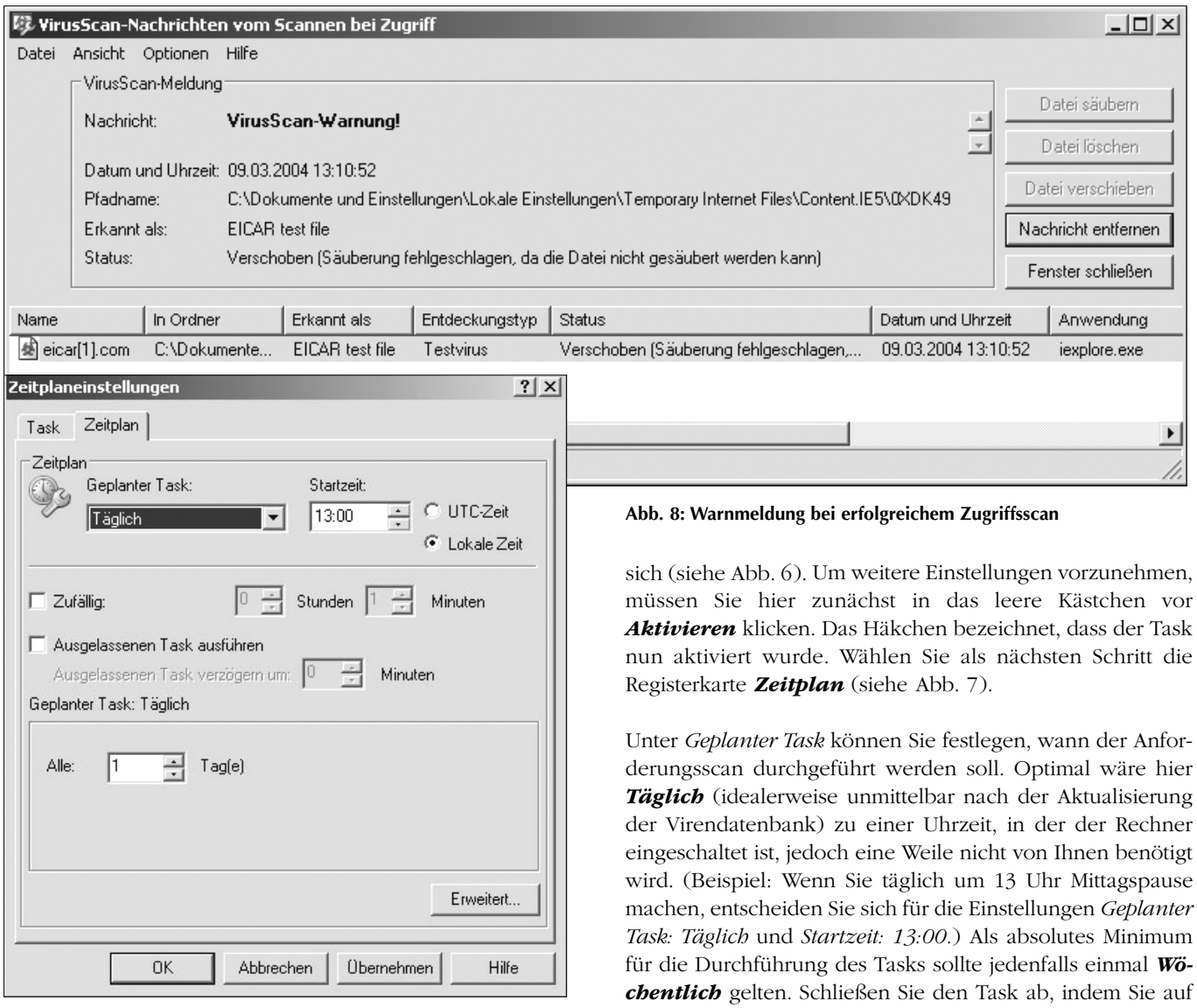

Abb. 7: Fenster *Zeitplaneinstellungen*, Registerkarte *Zeitplan*

Nachdem Sie sich mit den umfangreichen Konfigurationsmöglichkeiten vertraut gemacht haben und eventuell einige individuelle Adaptionen durchgeführt haben, schreiten wir letztendlich zum wichtigsten Kriterium: Und zwar zu jenem der regelmäßigen Durchführung des Tasks.

Garantieren können Sie eine solche regelmäßige Durchführung wiederum am besten mit Hilfe eines Zeitplans. Die weitere Vorgangsweise wird Ihnen schon wie Routine erscheinen: Kehren Sie im Fenster *VirusScan – Scannen auf Anforderung – Eigenschaften – Neuer Scan* auf die Registerkarte ***Ort*** zurück (siehe Abb. 5) und wählen Sie rechts mit einem Klick die Schaltfläche ***Zeitplan***. Sie sehen nun die Registerkarte *Task* des Fensters *Zeitplaneinstellungen* vor

Für Studierende ist McAfee VirusScan (Version 7.0) als Shareware unter `http://tucows.univie.ac.at/` erhältlich.

Abb. 8: Warnmeldung bei erfolgreichem Zugriffsscan

sich (siehe Abb. 6). Um weitere Einstellungen vorzunehmen, müssen Sie hier zunächst in das leere Kästchen vor ***Aktivieren*** klicken. Das Häkchen bezeichnet, dass der Task nun aktiviert wurde. Wählen Sie als nächsten Schritt die Registerkarte ***Zeitplan*** (siehe Abb. 7).

Unter *Geplanter Task* können Sie festlegen, wann der Anforderungsscan durchgeführt werden soll. Optimal wäre hier ***Täglich*** (idealerweise unmittelbar nach der Aktualisierung der Virendatenbank) zu einer Uhrzeit, in der der Rechner eingeschaltet ist, jedoch eine Weile nicht von Ihnen benötigt wird. (Beispiel: Wenn Sie täglich um 13 Uhr Mittagspause machen, entscheiden Sie sich für die Einstellungen *Geplanter Task: Täglich* und *Startzeit: 13:00.*) Als absolutes Minimum für die Durchführung des Tasks sollte jedenfalls einmal ***Wöchentlich*** gelten. Schließen Sie den Task ab, indem Sie auf ***Übernehmen*** klicken und mit ***OK*** bestätigen.

Punkt 4: Agieren im Vorfeld

Umsicht ist die beste Verteidigung

Kein Tormann vermag es, alle Bälle abzublocken. Ebenso kann auch die beste Antivirensoftware nicht alle viralen Attacken abwehren. Es verbleibt ein gewisses Restrisiko, das sich nur durch umsichtiges Handeln auf eine vernachlässigbare Größe reduzieren lässt.

Öffnen Sie deshalb prinzipiell keine eMail-Attachments unbekannten oder verdächtigen Ursprungs. Oft lässt sich bereits anhand des (nicht selten allzu „verlockenden“) Betreffs die (Un-)Seriosität des Inhalts abschätzen. Lassen Sie zudem Vorsicht walten bei Downloads aus dem Internet und achten Sie dabei stets auf namhafte Quellen. Weitere hilfreiche Ratschläge finden Sie im Artikel *Goldene Regeln für ein intaktes (Windows-)Betriebssystem* auf Seite 16. Im Zweifelsfall empfiehlt sich immer die alte Weisheit: *Vorsicht ist besser als Nachsicht.*

Verlängerung: Golden Goal

Der Fall der Fälle

Wenn Ihr Virenscanner erfolgreich ein Virus aufgespürt hat, erhalten Sie umgehend eine Meldung (siehe Abb. 8 auf Seite 25), die Ihnen mitteilt, wann und wo das Virus entdeckt wurde, um welches Virus es sich handelt und wie Ihr Virenscanner gegen den mutmaßlichen Angreifer vorgegangen ist (nachzulesen unter *Status*).

Keine Panik, Ihr Virenscanner hat bereits verlässlich das erste Krisenmanagement übernommen. Im dargestellten Fall hat er die Datei korrekt als *eicar testfile* erkannt und – wie in den Einstellungen festgelegt – in den Quarantäne-Ordner verschoben, weil eine Säuberung fehlschlug. Sollte auf Ihrem Rechner ebenfalls einmal die Situation eintreten, dass die Säuberung einer Datei misslingt, so empfiehlt es sich im Anschluss einen Neustart durchzuführen und die verschobene Datei erneut zu scannen. In den meisten Fällen wird dem Virenscanner die Säuberung nun gelingen.

Sollte dies nicht der Fall sein, ist es besser den Rat von Experten einzuholen, da die Alternative *Datei löschen* eventuell mehr schaden als nutzen könnte. Wenden Sie sich deshalb bei Fragen vertrauensvoll an unser Helpdesk-Team (eMail: `helpdesk.zid@univie.ac.at`, Tel.: 4277-14060).

Wenn Sie selbst überprüfen wollen, wie McAfee VirusScan arbeitet, können Sie unter `http://www.eicar.com/` ein Testvirus herunterladen. Das *eicar testfile* gibt es in mehreren Versionen: Als DOS-Programm, das zur Gänze aus einem ASCII-String besteht, als Kopie mit einem anderen Dateinamen sowie in einfach und doppelt gezippter Form. Ein guter Virenscanner wird das einfach gezippte „Virus" erkennen und vielleicht sogar das doppelt gezippte. Seien Sie unbesorgt, es handelt sich bei dem *eicar testfile* um kein „echtes" Virus, es enthält keinerlei Viruscode-Fragmente. Dennoch reagieren die meisten Virenscanner darauf, als ob es tatsächlich ein Virus wäre. Es eignet sich deshalb optimal für ein kleines „Freundschaftsspiel".

Michaela Bociurko ■

PS – speziell für jene, die einen neuen Rechner unter Windows XP in Betrieb nehmen wollen: Bedenken Sie, dass dieser bis zur Installation eines Antivirenprogramms völlig ungeschützt ist! Es empfiehlt sich daher, den Rechner während dieser Zeitspanne mit Hilfe der im Betriebssystem integrierten Firewall abzusichern. Eine Anleitung hierfür finden Sie im Artikel *Sicherheit von Anfang an – Windows XP mit Firewall-Schutz installieren* (siehe Seite 20).

RedHat Linux goes commerce

Die bereits Mitte letzten Jahres von RedHat angekündigte Auflösung der Standard-Linux-Softwareserie wurde nun endgültig vollzogen: „RedHat Linux" gibt es offiziell nicht mehr. Ab Ende April 2004 werden für RedHat Linux 9 keine Updates und keine Security Patches mehr bereitgestellt. Der Support für die älteren Versionen 7.x und 8.0 lief bereits mit Ende letzten Jahres aus.

Für die Nachfolge hat RedHat seine Produktserie in zwei Linien gespalten:

- Kommerziellen Support, kontinuierliche Updates, Bug- und Security-Fixes wird es hinkünftig nur mehr für die kostenpflichtige **RedHat Enterprise Linux (RHEL)-Serie** geben. Diese auf Unternehmenskunden abzielende Distribution gründet auf einer einheitlichen Code-Basis, was die Stabilität und Sicherheit verbessert sowie die Pflege vereinfacht. Lizenzpflichtige Enterprise-Versionen gibt es – je nach Umfang des Einsatzes – für Workstations, kleinere Server sowie für große Serverbetreiber. Eine Enterprise Linux AS Academic Edition kann um $ 50,– über den ZID erworben werden. Bei Interesse wenden Sie sich bitte an Peter Karlsreiter (eMail: `peter.karlsreiter@univie.ac.at`, Tel.: 4277-14131).
- Für die Weiterentwicklung der bisherigen Linux-Distribution hat RedHat die Quellen der Version 9 dem nicht kommerziellen Projekt Fedora übertragen. Das dort entwickelte freie **Fedora Core Linux** soll als Entwicklungsfeld für neue Linux- und Open Source-Technologien dienen. Fedora Core 1 ist seit November allgemein verfügbar, dessen Nachfolger, Fedora Core 2, bereits in der Testphase. Im Unterschied zu den Enterprise-Versionen kann es bei der Konfiguration eines Softwarepakets unter Fedora Core durchaus zu kleineren Fehlern im Rahmen eines Upgrades kommen. Größere Probleme gab es jedoch bisher nicht.

Fedora Core's tägliches Softwareupgrade mittels YUM

Bei Verwendung von YUM (*Yellowdog Updater Modified*) können Sie die tägliche Update-Funktion von Fedora Core mit den Befehlen **`chkconfig yum on`** und **`/etc/init.d/yum start`** aktivieren.

Da der Zentrale Informatikdienst der Universität Wien auf seinem FTP-Server einen Mirror der Fedora Core-Software hält, sollten Sie in der Datei `/etc/yum.conf` in der Rubrik `[base]` den `baseurl` auf den Wert

```
baseurl=ftp://ftp.univie.ac.at/systems/linux/
fedora/$releasever/$basearch/os
```

setzen. Analog sollte er in der Rubrik `[updates-released]` auf den Wert

```
baseurl=ftp://ftp.univie.ac.at/systems/linux/
fedora/updates/$releasever/$basearch
```

eingestellt werden. Dies erspart Ihnen unnötige Fehlschläge bei den Updates Ihres Betriebssystems.

Aron Vrtala