PATCHEN FÜR PROFIS

Windows-Hotfixes auch ohne *Automatische Updates*

In der letzten Ausgabe des *Comment* wurde das Windows-Dienstprogramm *Automatische Updates* vorgestellt, das sich selbständig auf die Suche nach neuen Security Patches macht und – falls es hierbei fündig wird – diese automatisch lädt und installiert (*Comment 04/1,* Seite 18 bzw. `http://www.univie.ac.at/comment/04-1/041_18.html`). In den allermeisten Fällen funktioniert das sehr gut; leider zeigt aber die Praxis, dass der *Automatische Updates*-Dienst nicht immer zu 100% zuverlässig ist. Die Gründe dafür können vielfältig sein – etwa eine zeitweilige Überlastung des Microsoft-Servers oder behindernde Einstellungen einer Personal Firewall. Um Sie vor unliebsamen Überraschungen zu bewahren, wollen wir Ihnen nicht vorenthalten, wie Sie Ihr Windows-Betriebssystem auch halbautomatisch bzw. manuell auf den neuesten Stand bringen können.

Die nachfolgenden Anleitungen beziehen sich auf die Systeme Windows XP und Windows 2000 (ab SP3), im Prinzip können die beiden Methoden aber auch für Windows 98SE, Windows ME und Windows NT (ab SP6) eingesetzt werden. Sie benötigen in jedem Fall eine Internetanbindung sowie einen Internet Explorer ab Version 5 (Download unter `http://www.microsoft.com/windows/ie/default.mspx`; mit älteren Versionen kann es eventuell zu Problemen kommen, da der Internet Explorer viele Installationsschritte selbst ausführt). Beachten Sie, dass die ActiveX-Funktionen des Browsers benötigt werden. (Klicken Sie dazu unter ***Extras – Internetoptionen*** – Registerkarte ***Sicherheit*** auf die Schaltfläche ***Stufe anpassen***. Beim Listenpunkt *ActiveX-Steuerelemente ausführen, die für Scripting sicher sind* muss ***Aktivieren*** ausgewählt sein. Bestätigen Sie hier mit ***OK*** und auf der Registerkarte *Sicherheit* mit ***Übernehmen*** und ***OK***.) Zudem müssen Sie mit den Rechten des Administrators arbeiten, um die Softwarekorrekturen installieren zu können.

Sind Sie geschützt?

Wird in den Medien von einem neuen Windows-Sicherheitsproblem berichtet, erfährt man oft nur, dass zu dessen Behebung eine Softwarekorrektur mit kryptischem Namen wie z.B. *KB835732* installiert sein muss. Wie aber können Sie überprüfen, ob der entsprechende Patch (etwa per *Automatische Updates*) tatsächlich eingespielt wurde? Ganz einfach: Wählen Sie ***Start – Systemsteuerung – Software*** und suchen Sie in der alphabetisch sortierten Liste der installierten Programme nach ***Windows Hotfixes***.

Sie finden hier alle bereits installierten Security Patches. Wenn Sie zudem erfahren möchten, welches Problem ein

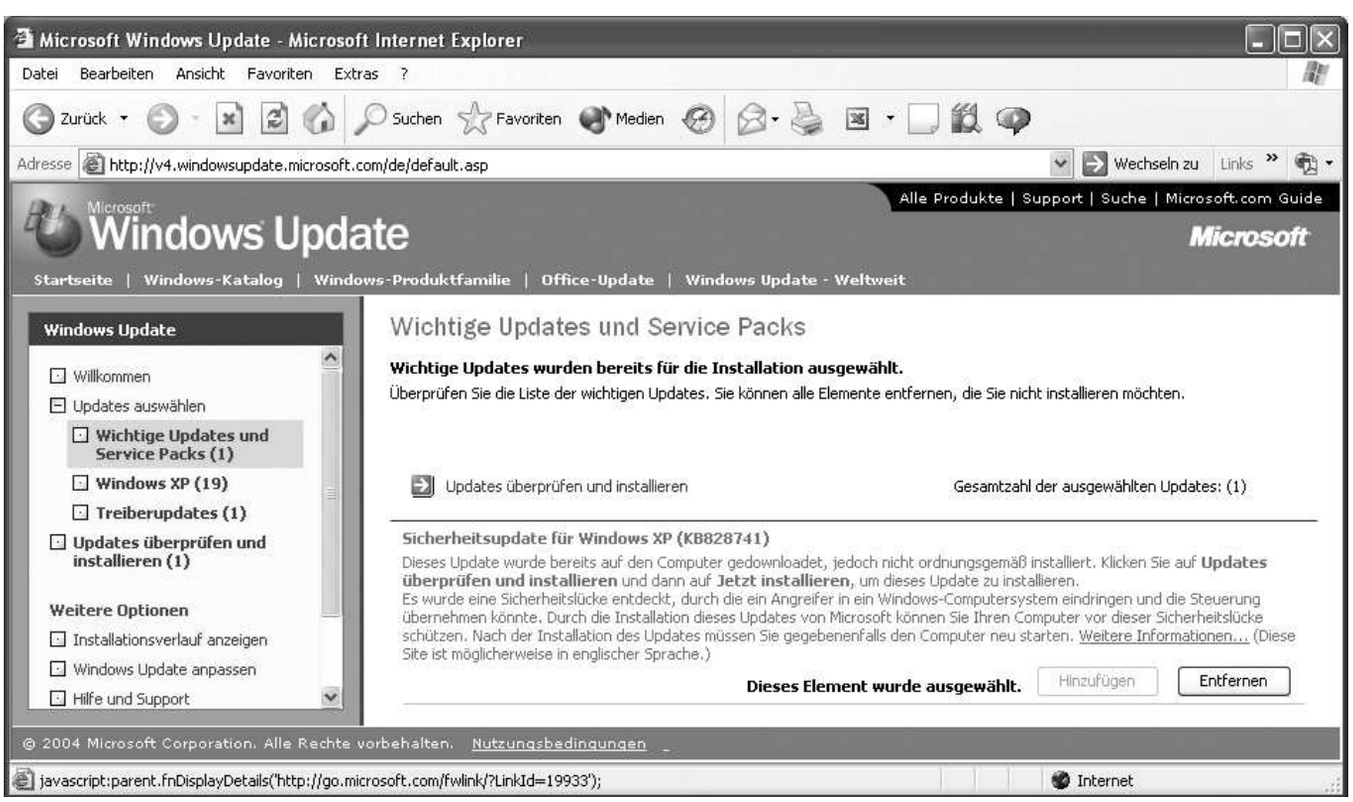

Abb. 1: Updates überprüfen und installieren

bestimmter Patch behebt, klicken Sie auf diesen und anschließend auf den Link ***Klicken Sie hier, um Supportinformation zu erhalten***. Sie werden nun direkt auf eine Webseite von Microsoft mit den benötigten Informationen verwiesen.

Patches halbautomatisch installieren

Eine mögliche Alternative zu automatischen Updates ist die halbautomatische Installation der notwendigen Patches. Wählen Sie dazu ***Start – Alle Programme – Windows Update***. Ihr Internet Explorer startet und lädt die *Windows Update*-Seite von Microsoft (alternativ dazu können Sie auch unter `http://www.windowsupdate.com/` auf die entsprechende Seite gelangen). Klicken Sie hier auf den Link ***Updates suchen***. Ein Diagnoseprogramm beginnt nun eine Abfrage auf Ihrem System, um herauszufinden, welches Betriebssystem Sie installiert haben und wann dieses zuletzt aktualisiert wurde. Basierend auf dessen Abfrageresultaten schlägt es Ihnen eine Auswahl wichtiger Updates und Service Packs vor (siehe Abb. 1 auf Seite 19).

Mittels der Schaltfläche ***Hinzufügen*** werden die erwünschten Elemente ausgewählt. Updates zu Programmen, die Sie nicht installiert haben, können Sie unbesorgt übergehen. Andere optional einspielbare Updates werden im Rahmen links zur Auswahl angeboten. Es empfiehlt sich, von Zeit zu Zeit auch hier nachzusehen, etwa wenn Sie einen speziellen Treiber suchen oder ein neues Feature von Microsoft installieren wollen. Nachdem Sie Ihre Auswahl abgeschlossen haben, klicken Sie auf den Link ***Updates überprüfen und installieren***.

Windows Update überprüft nun die Liste der zu installierenden Software auf interne Abhängigkeiten. Falls erforderlich wird eine bestimmte Installationsreihenfolge oder die Installation zusätzlicher Patches vorgeschlagen. Um die Installation zu beginnen, klicken Sie auf die Schaltfläche ***Jetzt installieren***. Windows lädt und installiert die benötigte Software; ein Fenster informiert Sie über den zeitlichen Ablauf. War der Vorgang erfolgreich, erhalten Sie die Meldung *Installation abgeschlossen* sowie üblicherweise die Aufforderung, einen Neustart durchzuführen.

Mögliche Ursachen von Fehlschlägen

Hin und wieder kann es leider geschehen, dass Updates nicht oder nur zum Teil installiert werden. Sie erhalten in diesem Fall eine entsprechende Meldung. Auf der *Windows Update*-Seite von Microsoft lässt sich durch Anklicken von ***Installationsverlauf anzeigen*** anhand des Status eruieren, welche Update-Aktionen erfolgten bzw. fehlschlugen. Diese Liste erweist sich auch als hilfreich, wenn Sie z.B. ergründen wollen, ab welchem Zeitpunkt automatische Updates fehlschlugen.

- **Patches wurden nur teilweise installiert:**
  Wenn besondere Abhängigkeiten von Patches untereinander bestehen, kann es sein, dass *Windows Update* nur einen Teil der aufgetragenen Aufgaben durchführt und anschließend einen Neustart verlangt. In diesem Fall sollte der beschriebene halbautomatische Vorgang wiederholt werden. Die bereits installierten Softwarekomponenten werden dann nicht mehr angefordert.

- **Patches wurden generell nicht installiert:**
  Eine denkbare Ursache wäre z.B. eine Überlastung des Microsoft-Servers beim Download. Diese kann durch Wiederholung der halbautomatischen Prozedur zu einer späteren Stunde oder am nächsten Tag umgangen werden. Es wäre aber auch möglich, dass Ihre Personal Firewall für ihr unbekannte *Windows Update*-Programme

Firewall-Zugriffsregeln für Windows-Updates

Damit *Windows Update* funktioniert, muss in der (Personal) Firewall zumindest für das Programm `svchost.exe` der Zugriff nach außen auf bestimmte Ports und Netzwerkbereiche freigeschaltet werden. Der Pfad zu diesem Programm ist davon abhängig, wo und wie das Betriebssystem installiert wurde (also z.B. `c:\windows\system32\svchost.exe`).

Geben Sie für das Programm `svchost.exe` folgende Regeln an:

Zugriff vom lokalen Rechner (`alle Ports`) über das Protokoll `TCP` nach außen (`outgoing`) auf die Ports `80` und `443` für die Netzwerkbereiche

- `207.46.0.0` mit Maske `255.255.0.0`
- `64.4.0.0` mit Maske `255.255.192.0`
- `213.199.144.0` mit Maske `255.255.240.0`

Bei der internen Firewall von Windows XP und bei der Norton Personal Firewall (diese ist Teil der Norton Internet Security Suite) sind keine händischen Änderungen nötig. Bei letzterer sollte der Zugriff allerdings auf die genannten Netzwerkbereiche reduziert werden, da die beiden mitgelieferten Regeln für *Generic Host Process for Win32 Services* zu allgemein gefasst sind.

Bitte beachten Sie, dass die hier genannten Regeln nur für das Programm `svchost.exe` gelten! Unter Umständen wird für das Update auch der *Windows Updater* (`update.exe`) geladen, der wieder eigene Zugriffsregeln benötigt. Im Bedarfsfall können Sie für die Zeit des Updatens den Zugriff aller Programme (also nicht nur `svchost.exe`) für die obigen Netzbereiche freigeben.

den Zugriff auf das Internet sperrt: *Windows Update* verlangt manchmal das Herunterladen eines speziellen Programms, das von der Personal Firewall dann oft automatisch blockiert wird. Es ist daher sinnvoll, für die Dauer eines Updates die Firewall rückfragen zu lassen, ob das Programm Verbindung mit den Servern von Microsoft aufnehmen darf. Bei den meisten Personal Firewalls ist diese Rückfrage ohnehin voreingestellt; bei der Tiny Personal Firewall z.B. lautet die entsprechende Funktion *Ask for action when no rule is found* (siehe dazu auch *Comment 02/2*, Seite 22). Eine Behinderung durch die Firewall sollten Sie keinesfalls durch Deaktivieren der Firewall beheben, sondern durch Freigabe der benötigten Kommunikationswege. Die erforderlichen Zugriffsregeln finden Sie im Kasten auf Seite 20.

Patches manuell installieren

Um die oben genannten Probleme zu umgehen, können Sie die Installation der erforderlichen Softwarekorrekturen auch manuell vornehmen. Ehe Sie diese Methode anwenden, sollten Sie sich jedoch ausführlich über den aktuellen Software-Versionsstand Ihres PCs informieren.

Auf der *Windows Update*-Webseite gelangen Sie durch Anklicken von ***Updates überprüfen und installieren*** erneut zur Liste der zu installierenden Updates und Service Packs. Wählen Sie beim fehlgeschlagenen Update den (nun grau dargestellten) Link ***Weitere Informationen***. Dieser verweist auf den technisch formulierten Sicherheitsbericht (*Security Bulletin*) zu dem betreffenden Patch. Dieser Bericht ist in den meisten Fällen nur auf Englisch verfügbar. Suchen Sie in der Liste die Überschrift *Affected Software* (siehe Abb. 2), wählen Sie dort die für Ihr Betriebssystem passende Software aus und klicken Sie auf den zugehörigen Link ***Download the update***. Dieser navigiert Sie auf die Download-Seite des jeweiligen Patches. Legen Sie hier die für Ihre Windows-Version zutreffende Sprache (in den meisten Fällen ***German***) fest und bestätigen Sie Ihre Wahl mit ***Go***. Die Seite wird nun in der von Ihnen ausgewählten Sprache angezeigt. Bei der hier angebotenen Software verrät das Ende des Dateinamens, für welche Sprachversion sie vorgesehen ist (z.B. `_DEU` für Deutsch). Laden Sie die gewünschte Datei herunter und führen Sie sie anschließend über Ihren Arbeitsplatz oder den Windows Explorer durch einen Doppelklick aus. Starten Sie im Anschluss Ihren Rechner neu.

Aron Vrtala ■

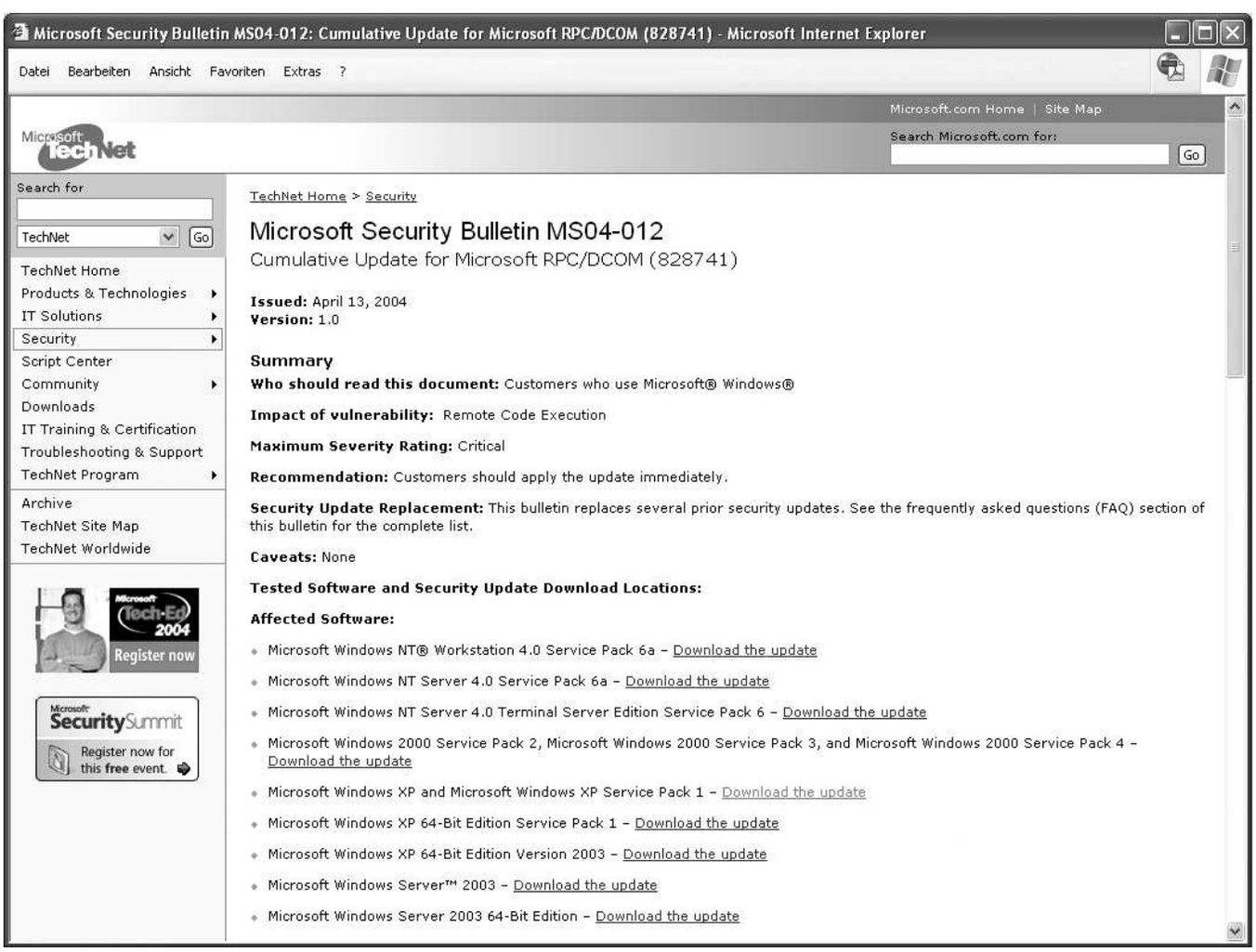

Abb. 2: Sicherheitsbericht von Microsoft

UNDE VENIS, NOTEBOOK, QUO VADIS?

Sicherheitsmaßnahmen für mobile Windows-Rechner

Herbst 2003. Ein Professor steht mit seinem funkelnagelneuen Notebook in einem Hörsaal der Universität Wien und präsentiert mit Hilfe von PowerPoint seinen Vortrag. Plötzlich erscheint ein neues Fenster am Bildschirm: Für alle HörerInnen sichtbar baumelt an einer Hand im Fenster ein Insekt, und es wird mitgeteilt, dass sich soeben der MS-Blaster-Wurm in das System einnisten wollte. Was war passiert? – Das Notebook hatte, was dem Vortragenden bis zu diesem Zeitpunkt nicht bewusst war, einen eingebauten WLAN-Adapter (*Wireless Local Area Network*), und der Hörsaal war über ein Funk-LAN an das Hörsaalnetz der Uni Wien angebunden. Die Systemsoftware des Notebooks war zwar frisch installiert, aber aufgrund der Zeitnot des Professors noch nicht mit allen Updates versehen. Glücklicherweise war bereits ein aktuell gehaltener Virenscanner installiert. Dem Notebook wurde automatisch über Funk-LAN eine Internet-Adresse aus dem Hörsaalnetz zugeteilt; es war also zum Zeitpunkt des Vortrags mit einer gültigen IP-Adresse im Netz registriert. Davon wusste der Vortragende jedoch nichts, denn er meldete sich im Hörsaalnetz nicht an. Leider befand sich im selben Netz auch ein Rechner, der mit dem MS-Blaster-Wurm infiziert war, und dieser versuchte das Notebook des ahnungslosen Professors zu befallen.

Woher kommst du, Notebook, wohin gehst du? Ein mobiler Rechner kann, wie im Beispiel oben, ohne Zutun seines Besitzers Gast in verschiedenen Netzwerken sein und ist damit unterschiedlich sicheren Umgebungen ausgesetzt. Deshalb ist die Systemsicherheit eines Notebooks besonders schwierig zu gewährleisten, obwohl sie aufgrund persönlicher Inhalte auf der Festplatte besonders wichtig ist.

Die Mobilität der Notebooks und die stetige „Seuchengefahr" im Internet erfordert heute eine immer größere Immunität der Geräte – nicht zuletzt deshalb, weil die Sicherheit eines Notebooks und des jeweiligen Netzwerks stets wechselseitig ist. Es ist nicht angenehm, wenn man mit seinem Laptop in fremden Netzen Schaden nimmt beziehungsweise Schäden verursacht: In beiden Fällen gibt es Aufsehen, Beschwerden, Erklärungsbedarf und Rückfragen, es kostet Zeit und kann (falls fahrlässiges Verhalten vorliegt) Regressansprüche nach sich ziehen. Eine besonders gute Visitenkarte stellt man sich mit dem Verbreiten eines Virus oder Wurms jedenfalls nicht aus. Gerade bei Notebooks ist daher – neben einer robusten Konfiguration – das richtige Verhalten des Besitzers entscheidend für die Systemsicherheit.

1. Aktuell bleiben

Ein Hauptproblem von Notebooks ist ihr variabler Zugang zum Internet und das daraus resultierende unterschiedliche Intervall für Updates der Virendatenbank Ihres Antivirenprogramms[1)] bzw. für den Download von Security Patches[2)]. Auf automatische Updates kann bei Notebooks nicht vertraut werden: Die sporadische Anwesenheit in Netzwerken garantiert keine regelmäßige Verbindung zu den Servern von Microsoft, Norton oder McAfee. Außerdem ist in manchen Netzen die Software-Aktualisierung gar nicht möglich. Wann immer Sie einen geeigneten Zugang zum Internet haben, sollten Sie daher vor dem Arbeitsbeginn Virendatenbank und Patches laden. Dies ist umso wichtiger, je länger Ihr Notebook nicht aktualisiert werden konnte. Verwenden Sie für Windows-Updates gegebenenfalls die halbautomatische Methode, die auf Seite 19 beschrieben ist. Über die Webseite `http://www.windowsupdate.com/` können Sie Ihr Betriebssystem regelmäßig aktualisieren. Generell gilt: Je älter das Update, desto größer die Gefahr.

Kontrollieren Sie darüber hinaus nach der Installation oder Deinstallation von Software oder bei Änderung Ihrer Netzwerkkonfiguration die Sicherheitseinstellungen Ihres Systems – speziell die der Firewall. Achten Sie auf verräterische durchgestrichene Symbole für den Virenscanner bzw. bei der Personal Firewall im Infobereich der Windows-Taskleiste (ausgenommen: die integrierte Firewall von Windows XP). Führen Sie sicherheitshalber hin und wieder ein manuelles Update Ihrer Virendatenbank durch.

2. Sauber bleiben

Auch bei jedem Datenaustausch sollte die Frage bedacht werden, wann das letzte Update von System und Virendatenbank erfolgte. Ein Virus ist über Bluetooth, Memory-Stick usw. schnell importiert. Angenommen, auf Ihrem Notebook wurden Betriebssystem und Virenscanner vor drei Tagen aktualisiert. Dann fahren Sie damit auf eine Konferenz, wo Sie vortragen, und überspielen die Daten Ihres Notebooks auf den angebotenen Konferenzrechner. Dafür verwenden Sie einen USB-Memory-Stick (einen „Schlüsselanhänger" mit Speicherplatz). Während des Überspielens infizieren Sie Dateien Ihres Memory-Sticks mit einem Virus auf dem Tagungsrechner. Wenn Sie später den Memory-Stick wieder an Ihr Notebook anstecken, ohne Ihr Antivirenprogramm aktualisiert zu haben, wird das Virus mit hoher Wahrscheinlichkeit auf das Gerät übertragen und kann dort ausbrechen.

Viel direktere Verbreitungsmöglichkeiten für digitales Ungeziefer sind die Kommunikationswege über Bluetooth oder Funknetze. Auch Firewire (IEEE 1394)- oder USB-Verbindun-

---

1) siehe Artikel *McAfee VirusScan – Ihr Goalkeeper im Einsatz gegen virale Offensiven* (*Comment 04/1*, Seite 21 bzw. `http://www.univie.ac.at/comment/04-1/041_21.html`)

2) siehe Artikel *Department of Desktop Security: Red Alert bei Windows-Betriebssystemen* (*Comment 04/1*, Seite 18 bzw. `http://www.univie.ac.at/comment/04-1/041_18.html`)

gen sind als Netzwerk betreibbar. Über Netze können Schädlinge nicht nur passiv – wie beim Memory-Stick – verbreitet werden, sondern aktiv das System zu befallen versuchen. Überlegen Sie bei Ihren Aktionen immer, welche Möglichkeiten Sie für die Übertragung von Computerschädlingen offen lassen, und beachten Sie dabei auch nicht konventionelle Datenträger wie Notepads, Organizer, Digitalkameras, Firewire-, Infrarot- und USB-Schnittstellen oder Handys. Blocken Sie – wo möglich – per Firewall alle netzwerkmäßig aktiven Schnittstellen vor einem Zugriff von außen.

Ein Notebook ist kein Server! In der überwiegenden Mehrzahl der Fälle ist es absolut nicht nötig, dass ein Notebook Dateien oder Drucker im Netzwerk anbietet. Mit dieser Einschränkung wird die Konfiguration einer Firewall sehr einfach. Unter Windows XP können Sie ganz leicht für jeden Netzwerkadapter eine Firewall betreiben: Unter ***Start*** – ***Systemsteuerung*** – ***Netzwerkverbindungen*** sehen Sie eine Liste aller verfügbaren Netzwerkverbindungen. Die nicht benötigten Verbindungen sollten Sie deaktivieren, indem Sie diese mit der **rechten** Maustaste anklicken und ***Deaktivieren*** wählen. Die Firewall für eine bestimmte Netzwerkverbindung wird gestartet, indem Sie diese ebenfalls mit der **rechten** Maustaste anklicken und ***Eigenschaften*** selektieren. Wählen Sie die Registerkarte ***Erweitert***, aktivieren Sie das Kontrollkästchen ***Internetverbindungsfirewall*** und bestätigen Sie mit ***OK***. Wiederholen Sie diese Prozedur für alle aktiven Netzwerkadapter. Für alle anderen Windows-Systeme sollten Sie eine Personal Firewall installieren und betreiben (siehe *Comment 02/2*). Unter Linux ist die Gefahr von Viren noch sehr gering; wenn Sie sich dennoch gegen unbefugten Zugriff schützen möchten, verwenden Sie am besten die integrierte IP-Tables-Firewall.[3)]

3. Wachsam bleiben

Eine gewisse freiwillige Selbstbeschränkung kann die Systemsicherheit drastisch erhöhen. Allerdings sollten die Maßnahmen mit Augenmaß gesetzt werden, weil damit natürlich auch ein Verlust an Funktionalität einhergeht. So ist es heutzutage nicht unbedingt ratsam, im Browser Java auszuschalten: Viele Webseiten wären dann nicht mehr verwendbar.

Einige generelle Regeln für richtiges Verhalten finden Sie im *Comment 04/1*.[4)] Die Gefahr, die von Trojanern ausgeht, sowie Möglichkeiten zur Erkennung und Beseitigung von ungebetenen Gästen sind ebenfalls im *Comment 04/1* beschrieben.[5)] Allen Notebook-BesitzerInnen seien zusätzlich folgende Verhaltensweisen besonders ans Herz gelegt:

- **Achten Sie auf aktuelle Informationen zu Viren, Würmern und Trojanern**, um das Bedrohungspotenzial besser einschätzen zu können. In den Medien wird heute zunehmend über Computerschädlinge berichtet. Warnungen vor akuten Problemen bietet die Homepage des ZID (`http://www.univie.ac.at/ZID/`). Aktuelle Querverweise zu Security-Informationen – z.B. zu den empfehlenswerten Sicherheitsnachrichten des RUS-CERT der Universität Stuttgart – finden Sie unter `http://www.univie.ac.at/ZID/security/`.

- **Seien Sie beim Öffnen von Dateien aus dem Internet generell defensiv!** Werden Sie umso defensiver, je länger Sie Ihr Betriebssystem bzw. Ihre Virendatenbank nicht aktualisieren konnten. Oft ist Bedachtsamkeit effektiver als rasches Handeln. Öffnen Sie daher per eMail einlangende Dateien nicht sofort. Word-Dokumente, PowerPoint-Präsentationen, HTML-Seiten, ZIP-Container, Bildschirmschoner, ausführbare Programme u.v.a.m. stellen heute immer ein gewisses Sicherheitsrisiko dar. Auch beim Browsen ist Vorsicht geboten: Microsofts Internet Explorer gilt (vor allem aufgrund seiner ActiveX-Funktionen) als besonders unsicher. Sie können die Gefahr deutlich verringern, indem Sie einen anderen Browser verwenden oder zumindest den Internet Explorer mit möglichst hohen Sicherheitseinstellungen betreiben.

- **Verwenden Sie, wo immer es möglich ist, Protokolle mit Verschlüsselung.** Netzwerke können generell abgehört werden. Bei Funknetzen ist zum Mithören aber nicht einmal ein physischer Zugriff auf das Netzwerk notwendig; darüber hinaus wird von den Funknetz-Betreibern oft keinerlei Authentifizierung oder Datenverschlüsselung eingesetzt. Für interaktives Arbeiten empfehlen wir daher SSH (*Secure Shell*) statt Telnet und FTP. Für eMail können Sie Webmail verwenden – damit werden die Webseiten verschlüsselt übertragen.

- **An öffentlichen Orten – Zug, Flugzeug, Bahnhof, Flughafen usw. – ist besondere Vorsicht angeraten.** Bluetooth-fähige Handys, deren Standardeinstellungen nicht geändert wurden, erlauben anderen Passagieren oft automatisch Zugriff (dasselbe gilt sinngemaß für PDAs und Notebooks, wobei letztere durch eine Firewall geschützt werden können und sollen). Sicherheitsmäßig sensible Dokumente sollten auch nicht in der Öffentlichkeit am PDA oder Notebook verarbeitet werden: *Top Secret*, *Geheim* usw. sind magische Wörter zur Steigerung der Aufmerksamkeit Dritter.

Also: *Unde venis quo vadis* – aus welchem Netz kommst Du und wohin gehst Du, Notebook, PDA, Organizer oder Handy? Mit diesem Gedanken im Hinterkopf und einigen Vorsichtsmaßnahmen lassen sich unvermeidliche Risiken der mobilen elektronischen Datenverarbeitung stark reduzieren.

Aron Vrtala ■

---

3) siehe Artikel *Hitchhiker's Guide to Security (Teil II) – Grundlegende Sicherheitsmaßnahmen für Linux-Rechner* (*Comment 02/2*, Seite 26 bzw. `http://www.univie.ac.at/comment/02-2/022_26.html`)

4) siehe Artikel *Goldene Regeln für ein intaktes (Windows-) Betriebssystem* (*Comment 04/1*, Seite 16 bzw. `http://www.univie.ac.at/comment/04-1/041_16.html`)

5) siehe Artikel *Ungebetene Gäste: Trojaner am Windows-PC* (*Comment 04/1*, Seite 10 bzw. `http://www.univie.ac.at/comment/04-1/041_10.html`)