AKTUELL: Sicherheitsmeldungen

Patch-Work

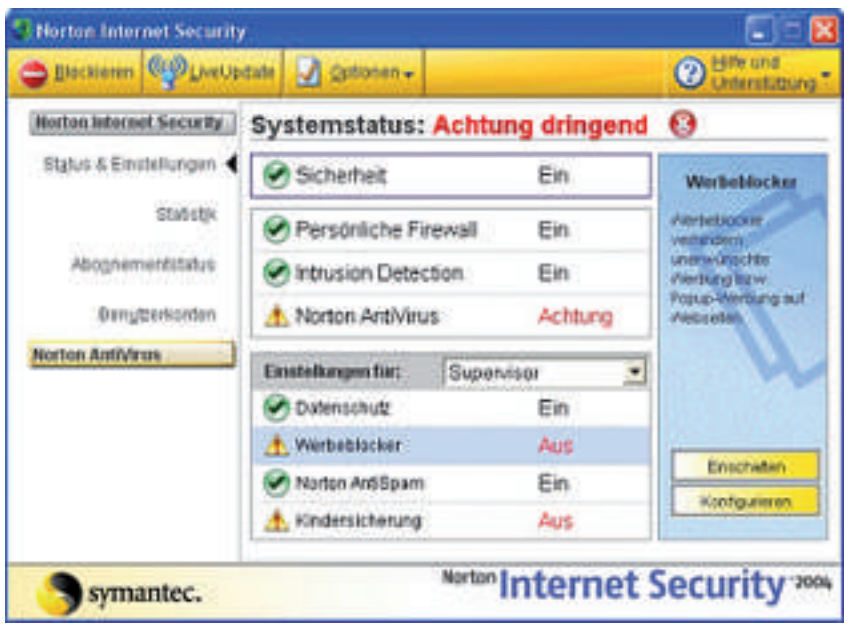
Nur mit den aktuellen Sicherheitspatches sind Ihre Programme auch wirklich vor der steigenden Flut an Malware, wie etwa Trojanern, geschützt. Panda meldet, dass die Zahl der Schadprogramme von 2000 bis heute von 1'000 auf 250'000 angewachsen sei.

Patch verfügbar

Lücke in Norton-Produkten

Symantec hat ein Update veröffentlicht, das eine gefährliche Lücke in den Produkten Norton Personal Firewall 2004 und Norton Internet-Security 2004 schliesst.

Der Besuch einer manipulierten Webseite und der Klick auf ein dort hinterlegtes Dokument führen auf ungepatchten Systemen zu einem Pufferüberlauf, über den Angreifer in der Lage sind, Schadcode auszuführen. Der Patch wird über das integrierte Live-Update heruntergeladen.
http://secunia.com/advisories/25290



Norton Internet-Security: Ein Patch schliesst eine gefährliche Lücke.

Microsoft

Neues Sicherheitsportal

Der Software-Konzern Microsoft hat ein neues Sicherheitsportal im Internet gestartet. Auf der bislang nur in Englisch verfügbaren Webseite bietet das Unternehmen aktuelle Sicherheitswarnungen und kostenlose Security-Downloads wie den Windows Defender an.
www.microsoft.com/security/portal

Google-Analyse

500'000 gefährliche URLs

Die Bedrohung aus dem Internet ist gewaltig: Bei einer Analyse des Google-Suchindexes wurden rund 500'000 Webseiten entdeckt, die versuchen, den PC eines Besuchers mit einem Schädling zu infizieren.
www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf

Microsoft

Update für Office 2003

Durch das Umwandeln von Office-Dokumenten in das neue XML-Format von Office 2007 soll sich eventuell vorhandener Schadcode entfernen lassen. Das Update namens Microsoft Office Isolated Conversion Environment (Moice) für Office 2003 setzt die vorherige Installation des MS Office Compatibility Packs für Dateiformate von Word, Excel und Powerpoint 2007 voraus. Weitere Informationen und Download-Adressen liefert die Microsoft-Knowledge-Base.
http://support.microsoft.com/kb/935865

Windows, Linux und Mac-OS

Open-Office-Wurm

Mit Badbunny ist ein Wurm aufgetaucht, der sich über Open Office verbreitet. Da er in der Starbasic-Makrosprache geschrieben ist, sind sowohl Windows-Nutzer als auch Linux- und Mac-OS-Anwender gefährdet. Badbunny versendet verseuchte Open-Office-Dokumente über die Chat-Programme Mirc und Xchat und verbreitet sich so weiter.

Soweit bisher bekannt, verfügt Badbunny über keine eigentlichen Schadfunktionen. Er sendet jedoch Ping-of-Death-Attacken an die Webseiten von Sicherheitsunternehmen.
www.sophos.de/security/analyses/sbbadbunnya.html

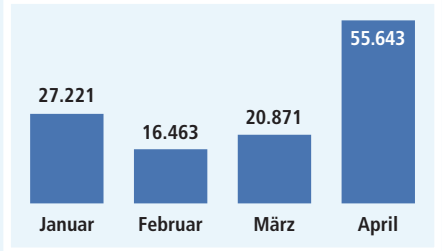
Phishing

Webbetrug nimmt zu

Während in den ersten drei Monaten dieses Jahres ein deutlicher Rückgang bei neuen Phishing-Seiten zu verzeichnen war, meldet die Anti-Phishing Working Group für den April einen massiven Anstieg. Allein in diesem Monat wurden mehr als 50'000 neue Seiten entdeckt, die versucht haben, Besucher etwa mit gefälschten Login-Seiten von Banken hereinzulegen um ihre Kontodaten zu stehlen.
www.antiphishing.org/reports/apwg_report _april_2007.pdf

PHISHING-WEBSITES 2007

Im April 2007 wurde die Rekordzahl von 55.643 neuen Phishing-Sites entdeckt.



Secunia Software-Inspector

Alte Firmen-Software

Bei einem umfangreichen Test mit dem neuen Network-Software-Inspector von Secunia wurde ermittelt, dass rund 28 Prozent aller Anwendungen in Unternehmen veraltet sind. Das Secunia-Tool kennt zirka 4'000 verschiedene Programme und prüft, ob die aktuellen Sicherheits-Patches eingespielt sind.

Für Privatanwender bietet Secunia den Software-Inspector an, der nach Sicherheitslücken unter Windows sucht. Der Online-Test auf der Webseite ist kostenlos.
http://secunia.com/network_software_inspector

Bug im Download-Manager

Patch für Opera

Die Opera-Version 9.21 behebt einen Fehler im Download-Manager, über den ein Angreifer einen Pufferüberlauf auslösen konnte. Dadurch war es möglich, über eine manipulierte Torrent-Datei Schadcode auf fremde Rechner einzuschleusen. Weitere Informationen sowie das Update sind über den folgenden Link erhältlich.
www.opera.com/docs/changelogs/windows/921

Windows-Update gehackt

Win-Update lädt Viren

Hacker haben herausgefunden, wie sich das von Microsoft verwendete Update-Verfahren für Windows dazu missbrauchen lässt, schädlichen Code aus dem Internet herunterzuladen.

Die Microsoft-Technik namens Background Intelligent Transfer Service (BITS) kann laut Symantec von einem bereits auf dem Computer vorhandenen Schädling gestartet und zum Download weiterer Komponenten genutzt werden. Der "Vorteil" dieser Technik ist, dass Windows-Update ein eigentlich gutartiger Prozess ist, der weder beim Anwender selbst noch bei Schutz-Software des PCs Alarm auslöst.
www.symantec.com/enterprise/security_response/weblog

Avira Antivir

Langer Pfad verhindert Updates

Wenn bei der Installation von Antivir ein Pfad gewählt wird, der 50 Zeichen lang oder länger ist, kann sich das Programm nicht mehr aktualisieren. Die Update-Komponente scheitert auf Grund einer falschen Parameterübergabe. Die einzige Abhilfe ist hier eine Deinstallation und anschliessende Neuinstallation nach einem Neustart des Computers.
http://forum.avira.de/thread.php?threadid=20936&page=7

Werbemüll hat sich verdoppelt

90 Prozent aller Mails sind Spam

Die Spam-Welle wächst immer weiter. Nach einem Bericht von Ikarus hat sich die Zahl der versendeten Spam-Nachrichten in den vergangenen zwölf Monaten verdoppelt und macht jetzt bereits 90 Prozent aller E-Mails aus. Besonders stark zugenommen haben in letzter Zeit Spam-Mails, in denen für den Kauf wertloser Aktien geworben wird, so Ikarus.
www.ikarus.at/statistiken/statistiken.htm

Windows-Update: Der Dienst kann von Schädlingen als Downloader missbraucht werden.

Updates bereits verfügbar

Zwei Fehler in Avast

Der Sicherheitsspezialist Nruns hat zwei Fehler in Avast entdeckt. Einem Angreifer war es möglich, durch manipulierte CAB- und SIS-Dateien Schadcode auf fremden PCs einzuschleusen. Ein Update wurde bereits über die automatische Aktualisierung verteilt.
www.nruns.com/security_advisory_avast_cab.php

Lücke im Internet-Explorer

Viele Websites infiziert

Das Sicherheitsunternehmen Avira meldet einen Angriff von Hackern, bei dem bereits über 10'000 europäische Websites infiziert worden sein sollen. Dabei schleusen die Angreifer über eine Lücke im Internet-Explorer einen unsichtbaren I-Frame auf den Webservern ein. Der Besuch einer infizierten Webseite führt dazu, dass ein Trojaner auf dem PC des Nutzers installiert wird.
www.avira.com

Youtube

Trojaner steckt im Film

Die Sicherheitsfirma Websense berichtet von einem Trojaner, der sich als Youtube-Video ausgibt und über E-Mails und Chat-Clients verbreitet wird. Die infizierte Datei zeigt ein Filmsymbol und spielt nach dem Öffnen tatsächlich ein Video im Browser ab. Im Hintergrund lädt das Programm aber zwei weitere Dateien aus dem Internet herunter, die private Informationen über den Nutzer ausspähen und weitergeben. Websense hat testweise den Virus aktiviert und gefilmt, was dann passiert. Dieses Video ist abrufbar unter **www.youtube.com/watch?v=pzKmzO_Xq3k** (in englischer Sprache).
www.websense.com

Videovirus: Ein Video von Websense zeigt, was der Youtube-Virus alles anrichten kann.

Trillian

Sicherheitslücke im Instant Messenger

Der weit verbreitete Instant Messenger Trillian der Firma Cerulean Studios weist einen Bug auf, der es Angreifern über manipulierte Nachrichten ermöglicht, eigenen Schadcode auf dem PC des Nutzers auszuführen. In der Version 3.1.6.0 ist der Fehler beseitigt.
www.ceruleanstudios.com

Server in Deutschland

Neues Botnet-Tool

Das Virenlabor von Panda Software hat eine Version des Trojaners Ld-Pinch entdeckt und so Hinweise auf einen deutschen Server erhalten, der ein neues Botnet-Management-Programm hostet. Ein Fenster des Tools zeigt die Zahl der infizierten Systeme nach Standorten an. Über das zweite, den Botnet Controller, kann der Angreifer Dateien herunterladen und abspielen, vordefinierte URLs blocken sowie Dateien auf FTP-Seiten hochladen, um sie wiederum auf betroffene Rechner herunterladen zu können.
www.pandasoftware.ch

Pufferüberlauf möglich

ActiveX-Lücke in Office

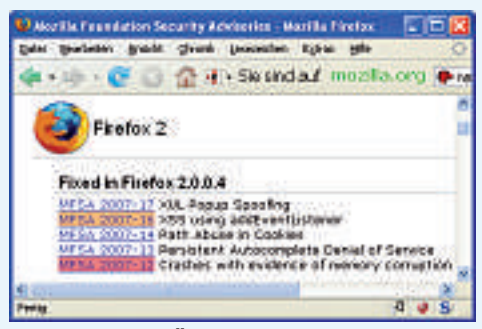
Ein ActiveX-Control in Microsoft Office 2003 enthält einen Fehler, mit dem Angreifer über präparierte HTML-Dokumente einen Pufferüberlauf erzeugen können. Symantec zufolge ist es damit möglich, Code einzuschleusen und zu starten, wenn der Nutzer auf manipulierte Websites surft. Betroffen sind Internet-Explorer 6 und 7. Microsoft untersucht die Lücke bereits.
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1260760,00.html *sel*

AKTUELLE WARNUNG: FIREFOX 2

Trotz frühem Firefox-Update gibt es immer noch eine Sicherheitslücke.

Obwohl die Entwickler mehrere Sicherheitslücken in Firefox 2.0.0.4 geschlossen haben, sei ihnen doch eine Lücke entgangen, berichtet Christopher Soghoian.

Laut Soghoian sind Angreifer in der Lage, schädlichen Code über den Update-Mechanismus einzuschleusen, den Firefox für Add-ons verwendet. Gefährdet sind Anwender, die Add-ons installiert haben, deren Download-Server nicht per SSL geschützt ist. Dazu zählen millionenfach installierte Extensions wie die Google-Toolbar und die Netcraft-Anti-Phishing-Toolbar. Bei dem von Soghoian beschriebenen Man-in-the-Middle-Angriff kommt eine Technik zum Einsatz, die als so geanntes Pharming bezeichnet wird. Dabei manipuliert der Angreifer das Domain-Name-System, so dass ein Download nicht von der korrekten Adresse, sondern von einem böswilligen Server erfolgt. Die einzige sichere Quelle für Firefox-Add-ons ist daher laut Soghoian derzeit **https://addons.mozilla.org**.
http://paranoia.dubfire.net/2007/05/remote-vulnerability-in-firefox.html



Firefox 2.0.0.4: Über das Update-System kann ein Angreifer gefährlichen Code einschleusen.