Redaktion WinTotal
Autor: PCDMicha@wintotal.de
alias Michael Appelt

SICHERHEIT IM INTERNET

Die jüngste Vergangenheit hat gezeigt, wie schnell man sich einen Virus einfangen kann. Nicht nur Privatanwender waren aber von der Attacke betroffen. Auch Firmen, die viel Geld für Virenschutz ausgegeben haben, hatten unter dem Virus „I Love you“ zu leiden. Die Erfahrung sollte allen eigentlich klar machen, dass Virenschutz und Sicherheit im Internet nicht nur einen Virenscanner, sondern auch gewisse Verhaltensregeln erfordert. Zudem macht die Standardinstallation vieler PCs den Viren und Trojanern das Leben relativ leicht, da ein Großteil der Nutzer Standardsoftware einsetzt.

Nur mit Virenscanner

Gefahren für den eigenen Rechner und die Dateien drohen aus unterschiedlichen Gesichtpunkten. Zum einen sind sogenannte Dateiviren noch immer im Umlauf und die häufigste Ursache für einen Virenbefall. Daneben gibt es sogenannte Trojaner und die boomenden Makroviren. Gegen all diese Virenarten schützen aktuelle Virenscanner ganz gut, welche mittlerweile zur Standardsoftware auf jedem Rechner gehören sollten. Eine Auswahl von kostenlosen Vertretern findet sich unter http://www.wintotal.de/softw/

Allerdings sollte den Virenscannern auch nicht blind vertrauen und jeden Dateianhang oder Download unvorsichtig öffnen, da die Scanner meist nur auf bekannte Viren reagieren können. Den besten Schutz gegen Makroviren (z.B. in Word-Dokumenten) stellen sogenannte Viewer dar. Microsoft bietet für alle Office-Applikationen ein Programm unter http://www.microsoft.com/germany/office/Office/viewers.htm an, mit welchem man die Dokumente öffnen und betrachten kann, ohne dabei die dazugehörende Applikation zu starten. Die Viewer führen keine Makros aus und bieten somit den besten Schutz. Eine sehr gute Alternative stellt auch ein universeller Dateiviewer wie Quick-View-Plus dar, welcher die Schnellansicht von Windows ersetzt und über 250 Dateiformate darstellen kann. Eine 30-Tage-Testversion dies Programms findet sich unter http://www.jasc.com/und kostet im Handel ca. 100 DM.

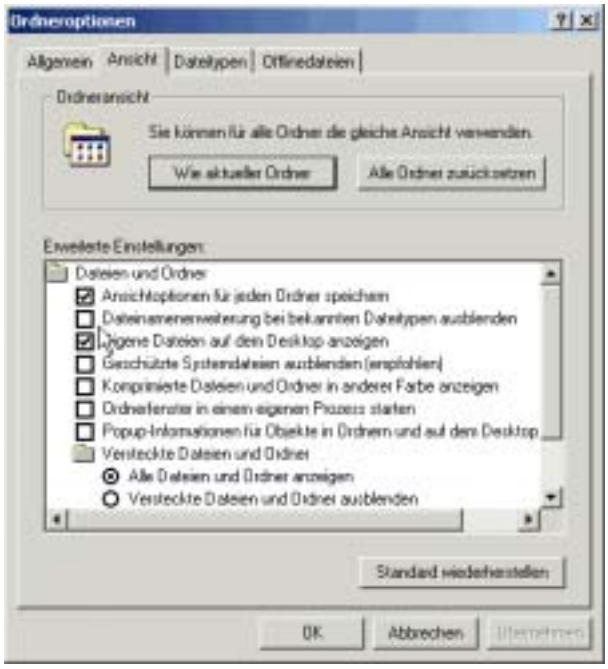
Aktive Inhalte

Gefährlicher sind aber die neuen Scriptviren. Hierzu gehört z.B. der bekannte „I Love you“-Virus. Diese benutzen den seit Windows 98 automatisch installierten Windows- Scripting-Host. Mit ihm ist es über eine einfache Programmiersprache möglich bestimmte Routinen des Betriebssystems und deren Applikationen direkt anzusprechen.

Die Scripte tragen die Endung VBS oder JS. Wer solche Dateien mit einem Doppelklick ausführt, startet damit das Script. Um die Endungen immer zu erkennen, sollte man im Explorer unter den Ordneroptionen bei Ansicht die Dateierweiterung auch für bekannte Dateitypen aktivieren. Nur so kann man erkennen ,um welchen Dateityp es sich eigentlich handelt, da sonst eine Verschleierung erfolgen kann. Die Datei bild.jpg.vbs wird ohne diese Umschaltung im Explorer als bild.jpg angezeigt. Anstatt bei einem Doppelklick auf diese ein Grafikprogramm zu öffnen, würde die Datei (anhand der Endung VBS, die ja nicht angezeigt

...

wird) mit dem Windows-Scripting-Host gestartet.



Da die meisten Anwender solche Scripte eh nicht benötigen, kann man den Scripting-Host über die Systemsteuerung-> Software-> Windows-Setup -> Zubehör entfernen und damit das versehentliche Starten solcher Scripte unterbinden.

Noch nicht sehr verbreitet, aber weitaus gefährlicher sind Scriptviren in HTML-Dokumenten. Mailclients wie der Outlook Express oder Outlook können Mails im HTML-Format anzeigen und erstellen. Diese können genaugenommen komplette Webseiten sein und auch aktive Inhalte beinhalten, die schon beim Anzeigen der Mail gestartet werden, ohne dass der Anwender überhaupt einen Anhang starten muss. Beide Mailclients orientieren sich bei den erlaubten Einstellungen für Webinhalte an den Vorgaben des Internet-Explorers und dessen Zonenmodell, da dieser intern zum Anzeigen der Mails verwendet wird. Erst die Einstellung „Zone für eingeschränkte Sites“ verbietet beispielsweise das Ausführen von ActiveX-Inhalten. Sowohl Outlook Express als auch Outlook bieten unter EXTRAS-Optionen-Sicherheit eine Funktion, um Webinhalte auf eine andere Sicherheitszone zu schalten. Beim Outlook schaltet man hierzu in dem Drop-Down-Feld "Zone" auf "eingeschränkte Sites".

...

Beim Outlook Express aktiviert man den Button "Zone für eingeschränkte Sites".

Was damit genau alles deaktiviert wurde, lässt sich in den Interneteinstellungen des Internet-Explorers (Systemsteuerung, Internetoptionen) unter Sicherheit einsehen und modifizieren, indem man die Zone "Eingeschränkte Sites" selektiert (ganz rechts) und unten dann auf Stufe anpassen klickt. Hier sollte man auch "active Scripting" und "AktiveX-Steuerelemente ausführen" deaktivieren. Dieses Dialogfenster lässt sich aus dem Outlook 2000 auch direkt aufrufen.

Benutzer von anderen Mailclients sind hiervon nicht betroffen, sofern diese nicht den Internet-Explorer als Modul zum Anzeigen der HTML-Mails benutzen.

Mite Juni hat Microsoft auf das Problem reagiert und stellt für Outlook 98 und Outlook 2000 unter http://officeupdate.microsoft.com/germany ein Sicherheitsupdate bereit, welches den Anwender vor aktiven Inhalten weitestgehend schützt.

Ob das eigene System sicher vor aktiven Inhalten in Mails ist, kann man unter http://www.heise.de/ct/antivirus/emailcheck/ prüfen. Die Zeitschrift ct versendet hier nach

...

Angabe der Mailanschrift eine Testmail, welche den eigenen Mailclient auf Scriptsicherheit hin überprüft. Weitere Infos gibt es unter dem Weblink.

Selbstverständlich gilt die Gefahr der aktiven Scripte in HTML-Seiten auch für das normale Surfen im Web. Wer allerdings hier alles restriktiv verbietet, wird im Web keine große Freude mehr haben, da ein Großteil der Seiten zur Navigation etc. aktive Inhalte benutzt. Sollte es dennoch erforderlich sein hier Anpassungen vorzunehmen, geschieht dies wieder in den Internetoptionen unter Sicherheit. Allerdings ist hier die Stufe für „Internet“ anzupassen.

Zuletzt empfiehlt sich ein Blick auf die Sicherheitsseiten von Microsoft unter http://www.microsoft.com/technet/security/current.asp, da hier alle aktuellen Sicherheitsprobleme im Zusammenhang mit Windows angesprochen werden.