heute.de computer

heute-Nachrichten
- Startseite
- Schlagzeilen
- Politik
- Magazin
- Wirtschaft
- Computer
- Sport
- Wetter
- Börse

ZDFmediathek

Sendung verpasst?
Jetzt ansehen

- ZDF heute
- ZDF heute journal
- ZDF heute nacht

Sendungen von A-Z

Service
- Podcast-Angebot
- heute-Telegramm
- Bildschirmschoner
- PDA-Angebote
- WAP-Dienste
- Newsletter
- RSS-Angebot
- Nachrichtenbanner
- Sidebar
- heute als Startseite

Auf Virenjagd mit Knoppicillin

Linux-Programm soll Windows-Nutzern gegen Schadprogramme helfen

von Alfred Krüger und Volker Heil

ZDF

Knoppicillin verspricht Hilfe für infizierte Rechner.

Die Antivirenfirma Sophos malt ein düsteres Bild von der Bedrohungslage im Netz. Die Gefahr, seinen PC mit einem Schadprogramm zu infizieren, sei im ersten Halbjahr stark angewachsen. Hilfe verspricht Knoppicillin, ein Virenjäger auf Linux-Basis.

Drucken Versenden 29.07.2007 [Archiv]

Vor 25 Jahren sah die Rechnerwelt noch völlig anders aus. Damals programmierte der 15-jährige US-Schüler Richard Skrenta den ersten bekannt gewordenen Computervirus und schickte ihn per Diskette auf die Reise von Rechner zu Rechner. Er wollte seine Freunde erschrecken, heißt es. Betroffen waren nur die damals weit verbreiteten Rechner der Marke Apple II.

Erster Virus war ein Scherzprogramm

Einen Namen hatte der erste Virus auch. Skrenta hatte ihn "Elk Cloner" getauft. Sein Schadpotenzial war gering. Der Schüler aus Pittsburgh hatte seinen Virus so programmiert, dass er jede Diskette, die in das Diskettenlaufwerk eines befallenen Apple-Rechners gesteckt wurde, mit einer Kopie seiner selbst infizierte. Bei jedem 50. Neustart des Rechners präsentierte er auf dem Monitor des Anwenders ein kurzes Gedicht. Darüber hinaus richtete der Virus keinen Schaden an.

Heute sind solche störenden, aber im Grunde harmlosen Schadprogramme die absolute Ausnahme. Auch die Verbreitungswege haben sich grundlegend geändert. Schadprogramme werden zwar immer noch auch über Wechseldatenträger wie CDs oder USB-Sticks in fremde Systeme geschleust. Die allermeisten Schädlinge kommen heutzutage jedoch über infizierte E-Mails und in wachsendem Maße über manipulierte Webseiten in den heimischen PC. Vielfach reicht schon der Besuch einer solchen Webseite aus, um den eigenen Rechner mit einem Schadprogramm zu infizieren.

Dabei ist es völlig unerheblich, auf welche Art von Webseiten man surft. Wurde früher besonders vor dem Besuch von dubiosen Seiten aus dem so genannten Dunkelweb gewarnt, so kann einen Surfer das Infektionsschicksal heute überall ereilen. Die modernen Schadprogrammverbreiter greifen gezielt Webserver an, auf denen Tausende Webseiten mit völlig "unverdächtigen" Inhalten gespeichert sind, und manipulieren diese Seiten. Je "unverdächtiger" die Inhalte sind, um so besser für die Schadprogrammverbreiter.

30.000 manipulierte Webseiten pro Tag

Die Zahl der manipulierten Webseiten stieg in den letzten sechs Monaten Sophos zufolge sprunghaft an. Im Juni dieses Jahres wurden fast 30.000 Webseiten neu infiziert - jeden Tag. "Das ist ein massiver Anstieg verglichen mit den 5000 Seiten pro Tag zu Jahresbeginn", heißt es im Halbjahresbericht der britischen Sicherheitsfirma zur Lage an der Cyberfront.

Kein Internetnutzer ist dieser Gefahr völlig schutzlos ausgeliefert. Virenscanner schützen zwar nicht vor allen Schadprogrammen. Ihr Einsatz minimiert das Risiko jedoch bereits erheblich. Die meisten Schädlinge, die man sich über manipulierte Webseiten einfangen kann, nutzen Sicherheitslücken in den gängigen Surfprogrammen. Dabei wird es immer unerheblicher, ob man mit dem Open-Source-Browser Firefox oder mit dem Internet Explorer aus dem Hause Microsoft durchs Netz surft. Wichtig ist, dass die benutzten Surfprogramme immer auf dem neuesten Stand gehalten und alle Sicherheits-Updates, die von den Herstellern regelmäßig angeboten werden, auch wirklich sofort installiert werden.

LINKS

Interaktiv
Computerviren - Vorbeugen und heilen

Eine hundertprozentige Sicherheit gibt es dennoch nicht. Selbst die schnellsten Sicherheitsfirmen brauchen immer eine gewisse Zeit, bis ihre Software auch vor den neuesten Schadprogrammen schützt, die gerade erst in die Umlaufbahn des Internets geschossen wurden. Ist ein solcher Schädling erst einmal im System, weiß er sich gut zu tarnen. Er verhält sich völlig unauffällig und versteckt sich irgendwo im Gewirr der Windows-Systemdateien. Antiviren-Programme schaltet der Schädling meistens ab. Dass mit dem PC etwas nicht stimmt, merkt der Nutzer meist nur daran, dass sich sein Rechner "irgendwie anders" als gewohnt verhält.

Schädlinge im System

Es gibt Indizien für einen Schadprogrammbefall, die auch dem Laien auf die Dauer nicht verborgen bleiben: Der Virenscanner lässt sich nicht mehr starten. Der Internet Explorer zeigt bei jedem Start automatisch eine unbekannte Suchseite mit Einträgen zu Potenzmitteln oder extrem billiger Markensoftware an. Das gesamte System arbeitet langsamer als sonst, und die Leuchtdioden des Routers blinken auch in den Surfpausen vor hektischer Betriebsamkeit. Das alles deutet darauf hin: Es ist ein Schädling im System.

Wer es genauer wissen will, hat ein Problem. Da der Virenscanner nicht mehr startet, lässt sich der Rechner auch nicht mehr auf Schadprogrammbefall hin untersuchen. Knoppicillin, ein auf dem freien Betriebssystem Linux basierendes Antivirenwerkzeug, könnte Abhilfe schaffen. Dreifach hält besser. Deshalb geht das von Klaus Knopper, Diplomingenieur der Elektrotechnik, entwickelte Diagnoseprogramm gleich mit drei namhaften Virenscannern der Firmen BitDefender, F-Secure und Sophos auf die Jagd nach Computerschädlingen.

Knoppicillin 5.2 befindet sich auf einer bootfähigen CD, die den Käufern des neuen "Security"-Sonderhefts der Computerzeitschrift c't als kostenlose Beigabe spendiert wurde. Der Rechner kann also mit dieser CD gestartet werden. "Die CD ist zwar kein Ersatz für einen vollwertigen Virenscanner", schreibt die c't. Sie helfe aber selbst dann noch weiter, wenn herkömmliche Virenschutzprogramme unter Windows nicht mehr arbeiten. "Knoppicillin ist unabhängig von den Daten auf der Festplatte und daher selbst dann noch lauffähig, wenn Schadsoftware Ihr System vollkommen unbrauchbar gemacht hat."

"Es kann scharf geschossen werden"

"Zur Virenjagd sind keine speziellen Linux-Kenntnisse erforderlich", heißt es in der c't. Tatsächlich wartet Knoppicillin mit einer selbst erklärenden grafischen Benutzeroberfläche auf, die auch ohne Vorkenntnisse einfach zu bedienen ist. Damit die Virenscanner auf dem neuesten Stand sind, muss über das Programm eine Internetverbindung hergestellt werden. Auch das ist meist problemlos möglich - es sei denn, der PC wird über einen USB-Funkadapter an einen WLAN-Router angeschlossen. In diesem Falle ist der Laie mit seinem PC-Latein recht schnell am Ende - ein Problem, mit dem offenbar auch die Vorgänger der neuen Knoppicillin-Version bereits zu kämpfen hatten.

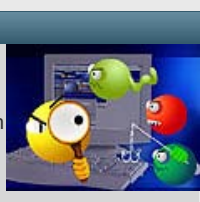
"Sollten die Scanner bei einem Suchdurchlauf tatsächlich auf ungewollte Schädlinge stoßen, kann auch scharf geschossen werden", schreibt die Zeitschrift und schickt eine Warnung hinterher. Knoppicillin gehe mit gefundenen Infektionsherden nicht gerade zimperlich um. Infizierte Dateien werden rigoros gelöscht. Im schlimmsten Fall könne es möglich sein, dass sich der Schädling in wichtigen Systemdateien eingenistet habe, ohne die der PC anschließend nicht mehr richtig starte.

Hilfe findet der selbst ernannte Viren-Jäger auf den Knoppicillin-Projektseiten des Computermagazins - und zwar auch dann, wenn er sein Windows nicht mehr starten kann. Die Knoppicillin-Programmierer haben ihrem Programm den Internetbrowser Firefox mit auf den Weg gegeben. Der Browser ist mit den Webadressen von Sicherheitsseiten und Virenlexika praktischerweise schon vorkonfiguriert. Wer Erste Hilfe braucht, wird also prompt bedient.

Drucken Versenden

zum Seitenanfang

ZDFmediathek



Interaktiv Computerviren - Vorbeugen und heilen
Fünf Schritte zum sicheren Rechner

zur ZDFmediathek

Externe Links
- Sophos Security Threat Report 7/2007 (engl.)
- c't - Projektseite Knoppicillin
- Skrentas Weblog

Das ZDF ist für den Inhalt externer Webseiten nicht verantwortlich

Mehr zum Thema
- Gefährliche Webseiten
  Immer mehr Schadprogramme werden über manipulierte Internetseiten verbreitet
- Keine Entwarnung im Netz
  Bessere Programme und härtere Gesetze sollen das Internet sicherer machen
- Lust auf Linux
  Knoppix, das Linux-Programm zum Kennenlernen, auf der CeBIT
- Steigende Bedrohung durch Trojaner
  (Un-)Sicherheit beim Online-Banking
- Cyberkriminelle Urlaubsgrüße
  Bundesamt warnt vor gefälschten Grußkarten-Mails

Suche in ZDF.de

Das Unternehmen | ZDFwerbung | ZDFshop | Zuschauerservice | Barrierefreiheit | About ZDF | tivi für Kinder

ZDFinfokanal ZDFdokukanal ZDFtheaterkanal arte 3sat PHOENIX KiKA Deutschlandfunk Deutschlandradio Kultur