

Virenstatistik 2008

So landen Viren auf dem PC

Der Antiviren-Spezialist Trend Micro hat sich die 100 meistverbreiteten Viren im Jahr 2008 angesehen und analysiert, wie sie auf den PC gelangen.

Downloads aus dem Internet stehen in der Auswertung von Trend Micro mit mehr als 57 Prozent an erster Stelle der Virenquellen. Ob es sich dabei um automatische Downloads – also ohne nennenswertes Zutun des Anwenders – handelt, oder ob der Nutzer auf einen Trick hereingefallen ist und den Schädling selbst herunterlädt, geht aus der Studie nicht hervor. Das Einschleusen durch andere Malware, die sich bereits auf dem PC befindet, ist der zweite große Verbreitungsweg (52 Prozent). Die Streuung per Mail spielt in Europa mit 5 Prozent eine geringere Rolle als weltweit (12 Prozent).

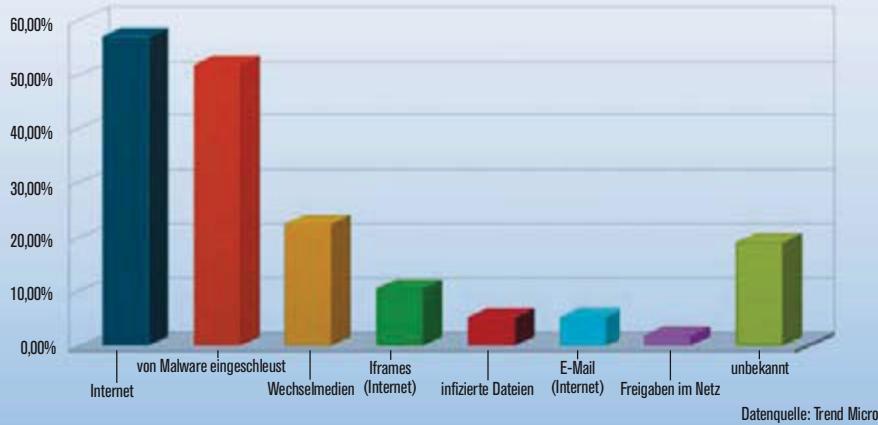
Wechselmedien sind erstaunlich infektiös: 22 Prozent der Schädlinge kommen auf USB-Stick & Co. zu ihrem Opfer.

Übrigens: Die Zahlen ergeben mehr als 100 Prozent, da sich die meisten Schädlinge auf mehreren Wegen verbreiten. Die Daten gelten für die 100 meistverbreiteten Viren in der Region EMEA (Europe, Middle East, Africa).

EINFALLSTORE Auf diesen Wegen schleusen sich Viren ein

Einfallstore der Top 100 Malware 2008

für die Region EMEA



Tipp: Rechnen Sie mit mehreren Schädlingen auf einem infizierten PC, denn 52 Prozent werden von bereits vorhandenen Viren ein-

geschleust. Wenn Ihr Antiviren-Tool einen Schädling meldet, lassen Sie einen Online-Scanner nach weiteren suchen. -fz/afa

Neue Angriffstechnik

Datenklau

Eine neue Technik namens In-Session-Phishing erfolgt nicht via Mail, sondern über ein Pop-up im Browser. Dabei wird ein weit verbreiteter Bug in der Javascript-Engine genutzt. Betroffen sind der Internet Explorer, Firefox, Safari und Chrome. Amit Klein, Chief Technology Officer beim Sicherheitsanbieter Trusteer, hat den Bug entdeckt. Wenn es Kriminellen gelingt, eine Internet-Seite zu hacken und dort den bösartigen Code einzuschleusen, erscheint das Pop-up. Es kann den Surfer etwa auffordern, Log-in-Daten samt Passwort einzugeben. Zwar muss der Angreifer sein Opfer auch hier von der Echtheit des Fensters überzeugen. Da das Fenster aber auf der passenden Site erscheint, wird es recht glaubhaft wirken. -bs

Frage des Monats

Sind Passwort-Manager in Browsern sicher?

Passwort-Manager bieten den Komfort, sich die Zugangsdaten für Websites wie soziale Netzwerke, Webmail oder Online-Foren nicht merken zu müssen. Sie füllen die Daten automatisch in die entsprechenden Formularfelder ein. Das Problem dabei ist nur, dass Angreifer diese Anmeldedaten stehlen können, indem sie den Browser mit Tricks dazu bringen, die Zugangsdaten in die falschen Formulare einzutragen.

Der Sicherheitsforscher Robert Chapin hat eine Studie veröffentlicht, in der er die Pass-

wort-Manager der gängigen Browser untersucht hat (über www.pcwelt.de/8dd).

Chapin hat die Tests mit dem IE7, Firefox 3.0.4, Opera 9.62, Safari 3.2 sowie Chrome 1.0 durchgeführt und in allen Browsern viele Fehler gefunden. Als Testsieger, wenn man das noch so nennen kann, gehen Opera und Firefox aus dem Vergleich hervor, weil sie immerhin jeweils sieben von 21 Tests bestanden haben. Der Internet Explorer kommt auf fünf, Safari und Chrome nur auf ganze zwei bestandene Tests. -fz

