

Microsoft Security Flaws Highlight Urgent Need for Personal Firewalls

John Pescatore

A stream of new Microsoft security flaws and the demands of patching them make the use of personal firewalls a critical enterprise requirement.

NEWS ANALYSIS

Event

On 9 July 2003, Microsoft issued three new security alerts that identified critical vulnerabilities in the Windows operating system and Windows-based applications.

Analysis

In little more than six months of 2003, Microsoft has issued twelve critical vulnerability alerts that require enterprises to patch every Windows-based PC. (More than half of these alerts have appeared in the past 90 days alone.) Most real-world hacker attacks focus on Internet-exposed servers, but the growing use of corporate desktops on broadband connections (whether cable modem service, digital subscriber lines or wireless LAN "hot spots") means that corporate PCs, particularly laptops used by remote workers, are more exposed to direct Internet-based attacks. Many of the recently identified vulnerabilities lend themselves to mass exploits via HTML-formatted e-mail, making scripted attacks likely — they require little technical sophistication.

Deploying the number of patches required by the Microsoft vulnerabilities to every corporate PC may take an enterprise six months or longer, and 18 months is not unusual. Moreover, Gartner believes that more Microsoft desktop vulnerabilities will be discovered in the immediate future. For this reason, system administrators should ensure that, at a minimum, every laptop in use — ideally every PC — has a personal firewall that limits exposure to Internet connections and keeps unauthorized executables from running. Internet Connection Firewall, built into Windows XP, is not sufficient because it blocks only incoming connections. Enterprises should also implement URL blocking products at the corporate firewall that maintain blacklists of URLs known to lead to sites that attempt to exploit these vulnerabilities.

Analytical Source: John Pescatore, Gartner Research

Written by Terry Allan Hicks, Gartner News

Recommended Reading and Related Research

- "Magic Quadrant for Personal Firewalls, 1H03" — Enterprises must install personal firewalls on remote devices that access their networks. **By John Girard**
- "Defining Intrusion Prevention" — Intrusion detection is fading away, replaced by intrusion prevention. **By John Pescatore and Richard Stiennon**

(You may need to sign in or be a Gartner client to access all of this content.)

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509