

Microsoft Sends Mixed Signals About Software Security

John Pescatore

Testimony given by a Microsoft senior executive doesn't seem to reflect Bill Gates' order to make security a top priority. Gartner agrees with Gates and believes that open source review would make Microsoft software more trustworthy.

NEWS ANALYSIS

Event

On 7 May 2002, Jim Allchin, Microsoft's senior vice president for Windows, told a U.S. federal court that computers running Microsoft software would be more vulnerable to attack if Microsoft had to disclose technical information to rivals so their software would work better with the Microsoft Windows operating systems (OSs). The nine states suing the software giant for antitrust violations have asked for this remedy.

Analysis

Allchin's statements in court do not seem to reflect Gates' directive to Microsoft employees to make security a top priority. On 15 January 2002, Microsoft Chairman Bill Gates issued a companywide memo that made the "Trustworthy Computing" initiative the top focus for his company. "Security models should be easy for developers to understand and build into their applications," he said. Gartner agrees with Gates and believes that open source review of Microsoft's code is necessary to meet security goals.

Computer hackers have had little difficulty breaking into Microsoft's closed-source software. A strategy of relying on security through obscurity (hiding source code) has already proven a failure for Microsoft. To make future products more trustworthy, Microsoft will have to become more expert at developing code that can withstand external review.

Gartner believes that open documentation and public review of program interfaces between OSs and applications will lead to stronger security mechanisms over the longer term (see *Research Note* SPA-11-3793 "Microsoft Breakup Would Reduce Malicious Content Impact"). Of course, attackers may exploit the exposed interfaces in the short term as the process brings to light existing yet undiscovered vulnerabilities. But this approach simply means that insecure code will become secure more rapidly and will therefore help Microsoft meet its goal of delivering trustworthy, secure software.

Only the courts will determine whether to impose this remedy for Microsoft's alleged abuse of its monopoly in desktop OSs. However, Gartner believes security does not offer a valid reason to reject making source code visible. Moreover, Gartner recommends that enterprises continue to weigh open source review as a positive factor in the security of software.

Analytical Source: John Pescatore, Gartner Research

Recommended Reading and Related Research

- "Microsoft Breakup Would Reduce Malicious Content Impact" (SPA-11-3793). Over the long term, the breakup and behavior remedies proposed for Microsoft would result in increased firewalling between PC applications and the Windows OS, thereby reducing the security exposure to malicious content. **By John Pescatore and Neil MacDonald**
- "Open-Source Software Doesn't Solve the Security Problem" (T-13-5678). Exposing source code to open review results in more rapid exposure and fixes of security vulnerabilities. **By John Pescatore**

(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