

The feds weigh in on Windows security

By Joris Evers

http://news.com.com/The+feds+weigh+in+on+Windows+security/2100-7348_3-6172158.html

Story last modified Mon Apr 02 06:22:15 PDT 2007

Will the White House make a difference in computer security?

The President's Office of Management and Budget recently sent out a directive to federal chief information officers to secure their Windows PCs. In what some said could have ripple effects well beyond Washington, the White House sent out a memorandum on March 22 that [instructed all federal agencies](#) (PDF) to adopt standard security configurations for Windows XP and [Windows Vista](#) by February 1.

"If the government states that it is only going to buy systems that are more secure, that sends a terrific signal," said Larry Clinton, president of the [Internet Security Alliance](#), a group that represents large corporate technology users. "It is a significant step. All the technology providers will now have to adapt their products to meet those standards."

Under the directive, technology providers who want to sell to the government will have to certify that their products work with specially-configured systems.

Locking down Windows PCs

The White House has ordered federal agencies to use standard security configurations on Windows XP and Windows Vista desktops by February. How are the feds going to do that? A sneak peek into the guidance:

For Windows XP:

- Use virus and spyware detection and removal utilities
- Use e-mail clients that filter spam
- Do not allow unapproved applications such as file-sharing and instant-message tools
- Run the system with limited user privileges
- Configure software to reduce exposure to threats
- Don't let Java, JavaScript and ActiveX applications launch by default

For Windows Vista:

Much of the same guidance applies, although Vista's default settings already take some of the XP tips into account. The [Windows Vista Security Guide](#) has additional technical guidelines on installation of Vista in a network.

"Common security configurations provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources," Karen Evans, an OMB administrator, [wrote in a memo](#) to federal CIOs on March 20.

According to Evans' memo, by adopting the standard configurations, federal agencies can improve system performance, decrease operating costs, and ensure public confidence in the confidentiality, integrity and availability of government information.

But at least one analyst described the move as just a minor development.

"On the one hand, every little thing matters; on the other hand, this is a little thing," said Pete Lindstrom, a Burton Group analyst. "Standard configurations are pretty obviously useful; global 2000 companies have been doing this for about 10 to 15 years now."

The Sans Institute, which specializes in computer security training, disagreed and instead applauded the government's move. The \$65 billion that the U.S. government is putting into IT purchasing each year will be an enormous incentive for technology providers to deliver products that work on secured systems, which will also benefit users outside the government, Alan Paller, director of research at Sans, [wrote on the organization's Web site](#).

"The benefits of this move are enormous: Common, secure configurations can help slow botnet spreading, can radically reduce delays in patching, can stop many attacks directly, and organizations that have made the move report that it actually saves money rather than costs money," Paller wrote.

The announcement arrives just as many developers are building applications for Vista, which means software companies can immediately work the requirements into their products, Sans said. To help technology vendors achieve this, the government plans in late April to make available copies of Windows installations based on the secure configurations.

Configurations for security installation have been developed by the [National Institute of Standards and Technology](#), the Department of Defense, the Department of Homeland Security, Microsoft and others. The U.S. Air Force has been a guinea pig in a "comply or don't connect" program with about 575,000 computers.

Microsoft first published its [Windows Vista Security Guide](#) in November, on the same day [it wrapped up work on Vista](#). A new version of the document was published in January after an [error was discovered in the earlier release](#). The error could cause some of the group policy objects not to be created correctly, Microsoft has said.

A security guide for Windows XP has been available since late 2005. The recommendations in the guide include running PCs without administrator privileges, not installing peer-to-peer or instant-message applications, and preventing automatic execution of applications common on Web sites such as Java, JavaScript and ActiveX.

The guide for Vista similarly provides instructions and recommendations designed to help strengthen the security of desktop and laptop computers running the latest Microsoft operating system, which is the most secure version to date, according to the software giant.

About two-thirds of successful attacks take advantage of misconfigured PCs and servers, according to research firm Gartner. The use of secure configurations out of the box has proven to be very effective, said John Pescatore, a Gartner analyst.

"This guidance by OMB is a very good idea," Pescatore said, noting that he reviewed and similarly commented on an early version of the directive.

But Burton Group's Lindstrom reiterated that the White House move will not exactly be a boon to security in general.

He cautioned that rethinking security configuration is not a panacea. "Presumably, there were a lot of reasons to have 'insecure' desktops in the past, so you don't just wave a magic wand and make it go away," he said.

But Sans is not deterred by such skepticism. The White House directive "reflects heroic leadership in starting to fight back against cybercrime," Paller wrote.

Now on News.com:

- [IBM adds low-wattage x86 servers](#)
- [Tech tips for parents of Web-surfing kids](#)
- [Rewriting ethics rules for the new media](#)
- [Extra: The 21 biggest technology flops](#)
- [Video: Mashups for all](#)

[Copyright](#) ©1995-2007 CNET Networks, Inc. All rights reserved.