La NSA colaboró en el desarrollo de Windows 7

www.npr.org/blogs/thetwo-way/2009/11/nsa_microsoft_windows_7...
por saulot el 21-11-2009 00:20 UTC, publicado el 21-11-2009 08:55 UTC

En una reunión de la Comisión de Seguridad y Terrorismo del Senado de los Estados Unidos, el Director de Seguridad de la Información de la NSA, la Agencia de Seguridad Americana, aseguró que la agencia había colaborado con Microsoft en el desarrollo de Windows 7. Vía MuyWindows: www.muywindows.com/2009/11/20/la-nsa-colaboro-en-el-desarrollo-de-wind/

NSA Is Giving Microsoft Some Help On Windows 7 Security

12:55 pm

November 17, 2009

comments (24)

Recommend (15)

A little help on security from the NSA. (Robyn Beck/AFP/Getty Images)

By Kevin Whitelaw

The National Security Agency has been working with Microsoft Corp. to help improve security measures for its new Windows 7 operating system, a senior NSA official said on Tuesday.

The confirmation of the NSA's role, which began during the development of the software, is a sign

of the agency's deepening involvement with the private sector when it comes to building defenses against cyberattacks.

"Working in partnership with Microsoft and (the Department of Defense), NSA leveraged our unique expertise and operational knowledge of system threats and vulnerabilities to enhance Microsoft's operating system security guide without constraining the user's ability to perform their everyday tasks," Richard Schaeffer, the NSA's Information Assurance Director, told the Senate Judiciary Committee in a statement prepared for a hearing held this morning in Washington. "All this was done in coordination with the product release, not months or years later in the product cycle."

The partnership between the NSA and Microsoft is not new.

In 2007, NSA officials acknowledged working with Microsoft during the development of Windows Vista to help boost its defenses against computer viruses, worms and other attacks. In fact, the cooperation dates back to at least 2005, when the NSA and other government agencies worked with Microsoft on its Windows XP system and other programs.

The NSA, which is best known for its electronic eavesdropping operations, is charged with protecting the nation's national security computing infrastructure from online assaults.

As these systems become increasingly dependent on private-sector computing products, the NSA has reached out to a growing number of software companies.

"More and more, we find that protecting national security systems demands teaming with public and private institutions to raise the information assurance level of products and services more broadly," Schaeffer said.

Schaeffer said that the NSA is also working to engage other companies, including Apple, Sun, and RedHat, on security standards for their products. The agency also works with computer security firms such as Symantec, McAfee, and Intel.

A growing array of law enforcement authorities, intelligence officials, and private computer experts has been warning about the rising threat of cyberattacks.

"The FBI considers the cyber threat against our nation to be one of the greatest concerns of the 21st century," Steven Chabinksy, the deputy assistant director of the FBI's cyber division, told the same congressional committee.

The Obama administration has been under pressure to name a cybersecurity chief to reinvigorate the government's efforts to protect its most sensitive computer networks. Some press reports suggest that appointment could come as early as next week.

Update at 5:30 p.m. ET: The text of Schaeffer's testimony, as prepared for delivery, is now online here.

Update at 2 p.m. ET: The NSA and other cybersecurity experts say that simple precautions (such as installing system updates regularly and running anti-virus software and firewalls) should protect against about 80% of the attacks out there. This means that if users took these steps, the NSA and others could focus on the more dangerous 20%, or so the theory goes. Put another way, of course, that means about 20% of attacks are sophisticated enough to theoretically defeat standard security measures.

(Kevin Whitelaw is a reporter for NPR.org.)