

'SQL Slammer' Lessons: Traditional Antivirus Is Not Enough

Arabella Hallawell

The fast-moving and damaging "SQL Slammer" worm shows that enterprises must re-examine all of their security practices and processes, not just their antivirus technologies, to protect against malicious-code attacks.

ANALYSIS

The staggering damage caused by "SQL Slammer" (also known as "Sapphire"), the fastest-spreading worm in computing history, shows that enterprises worldwide must re-evaluate their security processes and controls. Many enterprises, including some of the largest and most-prominent in the world, suffered crippling downtime that resulted in enormous costs to their businesses. Additionally, SQL Slammer exploited a security vulnerability — a buffer-overflow flaw that affects Microsoft's SQL Server and applications created with Microsoft Server 2000 Desktop Engine — for which a patch had been available for more than six months.

It is tempting to blame enterprise system and security administrators for not addressing this issue, but it is also unfair. Microsoft has released so many patches for security vulnerabilities in SQL Server — 11 patches from December 2001 to December 2002 alone — that administrators can't reasonably be expected to keep up with them all. System architects who chose to use products with many known vulnerabilities, and especially those who chose to expose these products to the Internet, also must bear responsibility for the havoc that SQL Slammer wreaked.

Enterprises primarily rely only on traditional antivirus products and processes to solve all types of malicious-code infections. They spend millions of dollars each year on antivirus software and internal processes designed to ensure that their desktop, file and e-mail server virus protections are updated regularly. However, these investments failed to protect against SQL Slammer, as well as the "Nimda" worm in 2001, which simply bypassed antivirus protections.

SQL Slammer and Nimda exploited well-publicized vulnerabilities in widely used server software. Antivirus products can't patch servers, and they should not be used for this purpose. In addition, they should not be installed on every server enterprisewide. Antivirus vendors may send early warnings of malicious-code attacks, and may advise enterprise personnel as to what steps to take to protect against the attacks. Other entities, such as security service providers and incident advisory organizations, also can perform this service. Security alerts offer limited protection against fast-moving attacks such as SQL Slammer and Nimda, which infected enterprise systems within minutes of their release.

The successful management of malicious-code threats is a more-complex enterprise initiative than simply installing and maintaining antivirus software with signatures issued by antivirus vendors. Organizational processes and effective governance decisions are more important than technology "fixes." One of the most important lessons of the SQL Slammer attack is that enterprises must make difficult policy decisions concerning what end users and IS organizations can, and can't, do with enterprise systems. In addition, decisions about which patches to distribute are not "black or white" judgments. Patching servers is costly and risky, and enterprises must make critical decisions about which patches are worth implementing, and when.

Patching the right servers and desktops, at the right time, is an overwhelming task for many large, distributed enterprises. Enterprises should focus their efforts on buying and deploying software products that do not require an endless series of patches. When this is not a practical option, the top priority for system and security managers should be to develop a risk model for patch management that's sensible for their enterprises, and to set up new governance and incident processes to ensure that this model is implemented effectively. These patch management processes should be accompanied by appropriate investment in server vulnerability assessment tools and services, as well as personal firewalls for desktops.

Enterprises also should evaluate the state of their perimeter protection. New technologies, such as application and personal firewalls, and desktop lockdown tools, should be implemented. Investment in new technologies and services should be judicious, however, and administrators

should not overlook the potential of traditional technologies. For example, asset management and network and systems management tools can address many patch management issues.

Enterprises that want to secure their systems must re-examine their defenses and vulnerabilities, and develop internal models and processes that work for their needs. This research is designed to guide enterprises in this process, and to ensure that they are protected against the next malicious-code attack — SQL Slammer was not the last.

"SQL Slammer' Lesson: Just Say No to Desktop Servers"

"SQL Slammer' Lesson: Patch Management Is Not Enough"

"Patch Management Benefits, Challenges and Prerequisites"

"Update Your Internet Server Security"

"Internet Security Metrics"

"Network Security Platforms Will Transform Security Markets"

"Deep Packet Inspection: Next Phase of Firewall Evolution"

"Expect Turmoil in the Enterprise Antivirus Market"

Arabella Hallawell

Editor in Chief

Security & Privacy

spotlight.feedback@gartner.com

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