

DATABASE BY DESIGN, INC.

Database Safety Issues Lessons learned from recent Internet attacks

Is Your Web Site Safe from Attack?

Do the answers to these questions keep you up at night?

- ✓ Is my data backed up consistently each day?
- ✓ Is the server secured so that malicious hackers aren't tempted to break into it?
- ✓ Does the software on the server have a vulnerability that makes it susceptible to attack?
- ✓ How do I know that the database and server are current with their software patches?
- ✓ Is my data safe?

We all want software to just work. Install it, turn it on, and let it go. Unfortunately, there are several issues that we, as users, need to monitor. Viruses can be handled automatically by virus protection software. However, since software isn't perfect, there will come a time when a bug is found that, if left alone, would place the computer in a compromising situation. Fixes for these problems often come shortly after they are discovered but they aren't automatically installed.

Why You Need to Check the Safety of Your Site

Usually when you have a database driven web site for your organization, you use a hosting service to manage your web site and database. This means that the hosting service will handle all the setup and maintenance of the server on which your web site resides. Therefore it is imperative that the hosting service stays current with all the software updates and patches to insure that the servers that hold your web site and database are running at peak efficiency. Depending on the software that resides on the server, this can be relatively easy or very time consuming and difficult.

Server maintenance is a time consuming and manual process. Tracking which software to patch can be a full time job. For instance, Microsoft has 57 security patches (more than one each week) for the last year (September 2002 - August 2003) listed on their web site to cover vulnerabilities in their software.¹ In order to demonstrate that server maintenance can be more difficult than it first seems, we will review the results of a devastating Internet attack that happened in January of this year (2003):



Anatomy of an Internet Attack

The "Slammer" worm (malicious software that copies itself to other computers) was launched on January 25 and designed to take over vulnerable computers on the Internet. The software targeted to accomplish the takeover was Microsoft's SQL Server - a database program used at many hosting services.

"The [Slammer] worm hit its first victim at 12:30 am Eastern standard time. The machine - a server running Microsoft SQL - instantly started spewing millions of Slammer clones, targeting computers at random. By 12:33 am, the number of slave servers in Slammer's replicant army was doubling every 8.5 seconds.."



"By 12:45 am, huge sections of the Internet began to wink out of existence...Three hundred thousand cable modems in Portugal went dark, and South Korea fell right off the map: no cell phone or Internet service for 27 million people. Five of the Internet's 13 root-name servers - hardened systems, all - succumbed to the squall of [transmission traffic]. Corporate email systems jammed. Web sites stopped responding...Emergency 911 dispatchers in suburban Seattle resorted to paper. Continental Airlines, unable to process tickets, canceled flights from its Newark hub."²

Microsoft SQL Server had a vulnerability that would let such a program take over the computer. Microsoft knew of the vulnerability and had a patch available to fix it. As evidenced by the dramatic results, hardly anyone installed the patch. One of the main reasons for not keeping up to date was that the process for installing the patch was quite involved and required the server to be down the entire time. With one computer, this might not be so bad. However, hosting services that use this software usually have tens, or even hundreds, of computers that each need to be updated.

The Bottom Line: Unsafe Systems Cost Money

In addition to the inconvenience of this attack, there was a substantial financial cost. Organizations lost productivity. They also had to endure the cost of clean up to remove the worm and fix its damage.

"London-based market intelligence firm Mi2g said that the worm caused between \$950 million and \$1.2 billion in lost productivity in its first five days worldwide...Technology market researcher Computer Economics estimates that the worm cost between \$750 million and \$1 billion to clean up."³

What You Can Do to Have a Safer Site

Even if you don't manage your web server and database system yourself, there are several things you can do to help you avoid falling victim to future attacks. Here are some questions you can ask your hosting service:



- 🔒 Ask for their update and patching policy. Make sure you are comfortable with it.
- 🔒 Ask how the software used for your web site and database compare in terms of security and safety compared to other software.
- 🔒 If you aren't comfortable with the software being used, ask if they offer other software options that you could use instead.
- 🔒 If none of the software options that are offered meet with your comfort level, find a new hosting service that offers software that has a safety and security history that is more to your liking.

Security and safety are very important to us at Database by Design, Inc. We strive to use software that has a history of being very secure and resistant to attacks. We also keep our software up to date, regardless of the time and cost to us, while at no cost to our customers. At Database by Design we want to ensure that your software will work well. Contact us so we can help you assess your Internet safety and stability concerns.

Database by Design, Inc. - (503) 579-4638

info@mycustomdatabase.com

<http://www.mycustomdatabase.com>

http://www.mycustomdatabase.com/newsletter_archives.html

(Previous Newsletters)

Next Month's Topic: Organize your data, organize your business - Tips for preparing your data for entering into a database.

References

- 1 "Security Bulletins", <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp>.
- 2 "Slammed!", <http://www.wired.com/wired/archive/11.07/slammer.html>.
- 3 "Calculating the Cost of Slammer", <http://zdnet.com.com/2100-1104-982955.html?tag=nl>.