Windows Manageability News & Analysis

Mark Minasi talks security, part two

More headlines

E-mail a friend

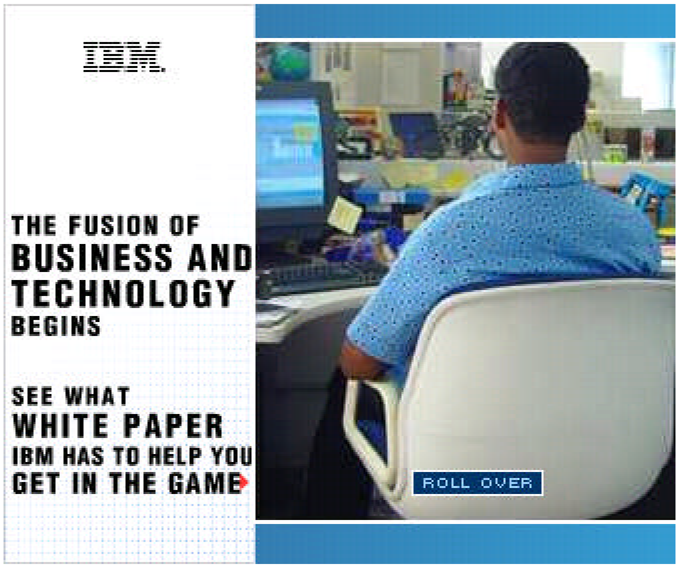
By **Christine Polewarczyk, Associate Editor**
09 Oct 2002, **SearchWindowsManageabilty.com**

Security is different in today's world -- there are no innocent bystanders anymore. Your systems might be protected, which would make you one of the good guys. Or they might be open to attack from worms that then use your system to broadcast worms to other systems, which would make you one of the bad guys.

In part one of this two-part series, we recapped Mark Minasi's sage advice, dispensed at the MCP TechMentor Conference in San Diego, on setting password policies, the dangers of the default administrator account, auditing and logs, disabling services and using split-brain DNS. Part two continues with more trenchant Windows security administration tips.

IIS: Adjust permissions; kill unnecessary functionality

Internet Information Server gets a worse rap that it deserves. If you make a few adjustments to permissions, kill unnecessary functionality and watch for and apply patches promptly, IIS can actually be a fairly secure server.



For permissions, consider that IIS is really nothing more than a file server. When a user hits a Web page, the person is really requesting the file called default.htm. Before visitors can see this file, they must receive authorization from NTFS and IIS. This is usually done through "anonymous logon." When the user accesses your IIS server named "X," that visitor is automatically logged in to your domain as user account named "IUSR_X." This is a potentially serious security issue.

One method for tightening things up is to set your entire Web server hard disk to "deny access" for IUSR, except for WINNT and wwwroot, which need read access. Keep in mind that while this helps secure IIS, it does not prevent buffer overflows, since they act as System when invading your Web servers.

To reduce unnecessary functionality, kill WebDav, Internet Printing, Samples, FrontPage junk, IISHelp and MSADC, if you can live without them. Also, using the IIS Lockdown from MS does help.

Take advantage of Windows 2000 security tools

There are several security tools that Microsoft (www.microsoft.com) offers to help automate your security processes. One is Secedit.exe, a command-line version of the Security Configuration and Analysis utility. You can use it to analyze and configure your computers based on security template settings. Secedit.exe allows you to craft logon script solutions for remote analysis and configuration of workstations within your enterprise.

Check out XP's software restriction policies

Use Windows XP's software restriction policies. XP includes a new set of Group Policy objects that allow you to allow or disallow applications based on application name, location, hash/checksum of a given file, a certificate, or an Internet zone (which you can use to prevent people from running ActiveX controls). These capabilities can give you a lot of power.

Don't forget physical threats

Internal threats can stem from disgruntled employees, on-site contractors with conflicts of interest, or anyone who might like to see or modify a piece of data on the network. They can also come from just plain old carelessness, stupidity and incompetence.

But internal security isn't just about account access and authorization. Physical access to your servers is something you need to consider as well. Keep people out of the room in which you keep your domain controllers. These days someone could pop off a server cover and hijack a hard drive in a matter of minutes, if not seconds. Or a person could have a malicious floppy disk in his pocket that he could easily slip into one of your server drives and then reboot. Perhaps these sound like farfetched scenarios, but why take the chance? Many attacks are much easier to perform locally than over the Net, including downing your server, cracking a SAM or your AD, stealing server hardware, and rebooting under DOS and reading NTFS files.

Get an SLA from your ISP -- ASAP!

Do you have an in-house service-level agreement (SLA) with your users? If you said yes, then you better have an SLA from your ISP too. You can't guarantee a quantifiable response time to your users if your ISP is not on your side. You need a promised response time from your ISP first.

Furthermore, you can't do much about "zombie" bandwidth-flooding attacks without your ISP's help. First, get an agreement on response time -- and then monitor it! If you're paying for the service, make sure you're getting what you pay for.

Don't be that guy

Don't help the jerks! Make sure your Web servers are Code Red-proof, so you're not unintentionally infecting others. Also, disable relaying on your SMTP servers so spammers lose their free mailers. Or better yet, if you can, disable the SMTP service (IIS).

You've heard it before: Educate your users

No matter how good your virus and macro filters are, there's always a way in -- but only if your users let them in. Spending just 15 minutes teaching your users about mail and attachments can go a long way.

Plan for the worst

Whether you're dealing with an internal or external security breach or a disaster-type situation, it's critical to have tested, step-by-step plans in place. Admittedly, this is not a small job, but it is absolutely necessary. You should also consider it essential training for new hires.

Stay informed and paranoid; use batch files to roll out hotfixes

Make regular visits to **microsoft.com/security**, which describes the latest hazards and offers the most current patches and tools. Also, use Microsoft's Software Update Service to apply patches automatically. And remember, there is no all-in-one security solution -- just because you have a firewall doesn't mean you're safe. Vigilance is your best protection.

Go back to **part one**.

LATEST NEWS

- >> **Microsoft mulling status of pilot programs** (eWEEK)
- >> **C# closer to ISO standardization** (CNET)
- >> **Outlook Express flaw rated critical for some** (IDG News)
- >> **Ballmer: No Microsoft markdowns** (Wininformant)
- >> **Survey: .NET will overtake Java next year** (InfoWorld)

WHAT'S NEW

on searchWindowsManageability

1. Webcast: Windows vs. Unix...
2. Know IT All Question of the Day
3. Microsoft's Trustworthy Computing
4. Security in wireless communications

Home | Search | News | Best Web Links | Books, Training & Research

About Us | Contact Us | For Advertisers | For Business Partners | Career Center Contacts

is part of the TechTarget network of industry-specific IT Web sites

APPLICATIONS
SearchCIO.com
SearchCRM.com
SearchSAP.com

DEVELOPMENT
SearchVB.com

NETWORKING
SearchNetworking.com

CORE TECHNOLOGIES
SearchDatabase.com
SearchSecurity.com
SearchStorage.com
SearchSystemsManagement.com
SearchWebServices.com
Whatis.com

PLATFORMS
Search390.com
Search400.com
SearchDomino.com
SearchHP.com
SearchSolaris.com
SearchWin2000.com
SearchWindowsManageability.com

TechTarget
The Most Targeted IT Media

TechTarget Enterprise IT Conferences | TechTarget Corporate Web Site | Media Kit

Explore **SearchTechTarget.com**, the guide to the TechTarget network of industry-specific IT Web sites.

Read our Privacy Statement