

Re: Seucity audit

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2004-03/0663.html>

From: Susan Bradley, CPA aka Ebitz – SBS Rocks [MVP] (*sbradcpa_at_pacbell.net*)

Date: 03/02/04

Date: Tue, 02 Mar 2004 12:38:04 -0800

Your security issues are not your server. Don't look there. It's your desktops. it's your employees. It's not "out there", it's "in here".

In SBS land that \$8,000 would be a waste of time because Foundstone would look at you from a corporate network "attitude".

In big server land, you assume people are sniffing your traffic, examining what information is bleeding off your connections seeing what patch level you are at. If you had posted in via a newsgroup versus the web interface I could have told you your external IP address that you posted from what version of newsreader you used. I could [with permission] fire packets at you using Foundstone's Superscan tool and told you what ports you had open. I could use nmap or any number of freely available tools what operating system you were running and through what hotfix you had installed. If you were not up to date on patches, I'd go to FullDisclosure or K-0tiks.com [or whatever that disreputable site in French is] and I'd download exploit code and fire it off at your unpatched system and nail you if the proper port was open in your firewall.

The reality is that none of this occurs in SBSland.

We get nailed from OUR stupidity because we don't patch and don't maintain.

You don't need to spend your security dollars on a security audit in SBS land. That's not where are risks lie out there.

1. What do "bots" see as your open ports? In SBS land we don't get hacked, we get stupid. Defcon hackers do not boast about taking down a SBS box. Go to grc.com click on shields up/ports up.. what ports are open. The fewer the ports, the less attack surface. Only open what you need, close what you don't.
2. What user rights are running on those workstations? I have to have a pretty loosey gooesy internal network to be "businessy" in my firm. I'm the only person running in "user" mode in my LAN, the rest are power

users or local admin. Local admin means they can accidentally install ANYTHING... so to counter that with

3. Trend SMB ... EVERY email that comes in the door is scanned and checked, I also quarantine zip files and what not. A/v on the server and the desktop and it checks for updates every hour on the hour.
4. Pop up blockers on Windows machines in the form of the Google tool bar
5. Plans to roll out XP sp2 as soon as it hits the streets [lots of security features].
6. Get 100% Windows XP office so that at a moments notice I can patch ALL workstations – if you have one Windows 98 in the LAN you have no security.
7. Save your money on that audit and buy www.shavlik.com HfnetchkPro and be able to remotely from your desktop [or the server] patch the server and all XP workstations with one button.
8. Ensure that all laptops have antivirus/patching/firewall as well. Set up a procedure where standalone laptops are "checked in and checked out"
9. Do you have employee manuals that cover authorized and unauthorized internet and email use? {Policy first and foremost}
10. Buy employees a copy of Trend Micro's pccillian for home use, require that they load it up.
11. Sign up for Microsoft security bulletins and ensure you get notified. Patch in a timely manner.
12. Have monthly employee awareness meetings training people to "not just click"
13. Alarm on the building.
14. Good tape backup with rotation off site.
15. Kensington physcal cable locks on computers in the office to slow burglars down.

There... I'll bet you those steps don't cost \$8,000 and I just gave you action items rather than giving you a security audit that would tell you that you have weaknesses and then you'd have no budget to do anything about them.

I'll send you a bill.

A can of Mountain Dew and a promise that you'll hang around this newsgroup. :-)

Susan

Roger wrote:

- > *Thanks... those are all great tools.*
- >
- > *Depending on the costs... I'd consider a full blown*
- > *security assesment from a company to evaluate my*
- > *infrastructure, and even exploit the vulnerabilities they*
- > *find within...*
- >
- > *So far, I haven't found a company that's cost effective.*
- > *These evaluations are looking to be better then 8k!*
- >

--

<http://www.sbslinks.com/really.htm>