
Steps to Take to Ensure That Your Network Is Secure

Contributed by Webmaster
Friday, 27 November 2009
Last Updated Friday, 27 November 2009

By Roberto Garabell

Hacking and computer crime isn't a hobby, nor is it a profession. It is more like an obsession, and computer criminals never take a day off. Every minute of every day, thousands of them are scouring the Internet for those proverbial "back doors" (and the growing number of side doors) to other people's networks. There are a number of steps to take to ensure that your network is secure.

Of course, if you or your firm has big enough budget, your computer specialist, security staff or IT consulting company can devise a 24/7 plan that will take care of you. On the other hand, most individuals and many companies don't have that kind of budget, so you need to take some planned, programmed and regularly scheduled steps to provide maximum protection for your network.

Daily duties

Protecting your network is a constant, continuous responsibility, requiring daily diligence. It's less difficult than you think to develop a common sense, straightforward task list to secure your network. To get you started-your final list may be shorter, longer, the same or very different than ours-here are a number of steps that are common to many network security plans.

Start the day (and end it, too, for extra safety) by checking your network traffic statistics. If there was more than the usual minimal traffic at night, and an extraordinary amount during the day, you need to find out what type it was. Look far enough to find out the destinations and sources.

Also check the security logs from your domain servers to see if the system is locking out any accounts, and pay extra attention to any that have administrator access. Make sure any lockouts were simple human error rather than a coordinated attack.

Now move on to your antivirus logs to see if any viruses your system since your last check-up. While you're at it, make sure your antivirus profiles (or "signatures") are current and installed.

A last log check: Take a close, careful gander at your IDS and firewall logs. If someone on the Internet is lurking around your door, you need to know about it. Often, such activity indicates that someone inside your network may be up to some activities, purposely or not, that they should be avoiding.

If any of your log checks shows unauthorized or illegal activity occurring, report it at once, of course, then take corrective action to stop similar activity in the future. You might also give some thought to the question, What are they looking for?

Have regular "meet and brief" sessions with managers and other employees who need to know what's happening with your network and computers. Review any actions that have been taken recently. In these get-togethers, everyone should feel free to ask questions and offer new ideas.

Now that you have an idea of what unapproved activities may be occurring, and have discussed it with the appropriate people, turn knowledge into action. Change firewall rules consider archiving logs to save server space and update all administrator privileges.

Generally speaking, you want to "tidy up and tighten up." This includes ensuring that you always have the latest security patches. If new ones are available, get them, install them, then read the release notes-twice.

Verify current connections at random times, day and night, weekdays and weekend. If you can spot malicious behavior while it's happening, you will save a lot of time. Also make sure to check every connection going through your network firewall, both inbound and outbound, and watch out for anomalies of any kind or size. Investigate everything, including outbound FTP traffic, inbound Telnet/SSH sessions or anything else that isn't quite "normal" or expected.

The "semi-summary"

This is a "semi-summary" because you have to write the end of this tale yourself. Not every small business or home office can run a 24/7 security operation, and some may only have a single person available or qualified for the work anyway. The best way to keep from missing things and making mistakes is to make a daily checklist (some things can be done weekly, too) and following it precisely.

Network security is much more powerful when it's preventive and pro-active, rather than reactionary. Don't wait for things to happen-because they will, and you will be fixing things more than protecting them. Make your list, keep it updated, stay current on security issues and don't get careless or complacent. If you follow your own rules, however you develop them to fit your particular situation, you will most likely avoid the worst, biggest attacks and prevent scores of smaller ones. You need to invest some time, but the payoff is huge.

Visit Data Source.net for LA computer repair where we specializing in the design and implementation of high end digital networks and also provide computer repair/recycling in Orange County LA. Visit online today.

Computers And Technology

{mos_sb_discuss:2}