10 things you can do to improve network and PC security

Takeaway: Securing your network and PCs is a never-ending battle. Here are some effective strategies to add to your arsenal.

Security. It's that which drives some administrators to early retirement, gray hair, or a permanent room in a padded cell. Okay, that's an exaggeration… but you get the idea. Security is tops on most every administrator's list. And with good reason. Incomplete or poor security can bring down a company's network and/or computer resources. That equates to lost work, which affects bottom line.

Administrators must do all they can to ensure the security of their networks. But for some (especially those without the financial resources), just knowing where to start and what to use is the biggest challenge. With that in mind, I thought I'd lay down 10 tools and methods to help you arrive at better network/PC security.

1: Use Linux

I can already hear the groans from the gallery, but the truth of the matter is, you will cut down on PC security issues if you begin migrating at least some of your desktops to Linux. The best way to do this is to migrate users who don't require the use of proprietary, Windows-only applications. If you use Exchange, just make sure you set up OWA so that the Linux users can access Web mail. Migrate a quarter of your desktops to Linux and that's a quarter fewer security risks you'll have to deal with.

2: Block users from installing software

I've had to deal with companies that do this. Yes, it can be a pain when users actually need a piece of software installed (you'll have to visit their offices just to enter the administrator credentials), but the dividends it pays off are significant. You'll have far fewer viruses and less malware to deal with than you would if the users were allowed to install at will. The give and take is certainly worth it here.

3: Upgrade your antivirus

I'm always shocked when I see antivirus tools that are out of date. This goes for applications and virus definitions. When dealing with the Windows platform, it's crucial to keep everything as current as you possibly can. Keeping antivirus up to date is the only way to help protect vulnerable machines from malicious software and files.

4: Switch your browser

Not to stir up the mud, but the truth of the matter is simple: Internet Explorer is still an incredibly insecure browser. One of the best things you can do is migrate your users from IE to Firefox. Yes, Firefox may be getting a bit bloated, but it's still far more secure than the Windows counterpart.

5: Disable add-ons

Browsers and email clients make use of add-ons. Some are necessary for work — some are not. Those that aren't needed should not be used. Although some add-ons offer some handy features, it's not always possible to ensure the validity or security of an add-on. And even when you can, it's not always a given that the add-on won't affect the performance of the machine. I've seen plenty of Outlook, IE, and Firefox add-ons drag a machine to a screeching halt.

6: Deploy a hardware-based firewall

Let's face it: The built-in Windows firewall is simply not sufficient. If you want real security, you need a dedicated firewall on your network. This firewall will be a single point of entry that will stop many more attempted breaches than the standard software-based firewall will. Besides, the hardware-based fire will be far more flexible and customizable. Look at a Cisco, Sonicwall, or Fortinet hardware firewall as your primary protection.

7: Enforce strict password policies

For the love of all things digital, don't let your end users control their password destiny. If you do this, you'll wind up with accounts and systems protected with "password", "1," or worse — nothing at all. Make sure all passwords require a combination of upper/lowercase, numbers and letters, and special characters. While you're working on password policies, be sure you enforce a rule that passwords must be changed every 30 days. It's an inconvenience, but it's worth the security it brings.

8: Do not share networked folders with "Everyone"

Although it's tempting (especially when you can't figure out why a user can't access a folder), do NOT give the everyone group access to a folder. This just opens up that folder to possible security issues. If this becomes an absolute necessity, only do it temporarily. For security's sake, spend the extra time troubleshooting why that user can't access the folder, instead of just giving everyone full access.

9: Use network access control, like PacketFence

PacketFence is one of the most powerful NAC tools you will find. With this tool, you can manage captive-portal for registration and remediation, and you have centralized wired and wireless management, powerful guest management options, 802.1X support, layer-2 isolation of

problematic devices, and much more. With this system on your network, you can rest assured that rogue devices will have a much smaller chance of connecting.

10: Use content filtering to protect from malware

I'm not a big fan of posing as Big Brother, so I don't advocate too much content filtering. I do, however, believe it's valid to use content filtering to prevent malware. There are obviously certain phrases, keywords, and URLs that can and should be filtered, based on their history of causing malware. I won't post the best keywords to filter for malware, as those words might land me in trouble. Just do a simple search for keywords associated with malware.

Other tips?

Securing your network and PCs is a constant battle. But with the right tools and strategies, your network can be a much safer arena for productivity. Give a few of these options a look and see if they offer the missing pieces needed to further secure your environment.