

# Bangkok Post

## database

February 23, 2005

### NETWORKING / 10 STEPS TO A SAFER COMPUTER ENVIRONMENT

## Rules for setting up an almost perfectly-secured LAN

by LOUIS MENTHON

Faultless network security remains as elusive as ever and it is nearly impossible to completely secure a LAN since a lot of factors come into the picture. I would say "network security is as strong as your weakest link." You will find below a list of non-exhaustive rules. I could have added certificates, VPN, biometrics, radius server, IDS, IPS plus other methods to harden and secure a network, but the subject is endless and space is limited.

Probably the weakest security link is the human factor. No matter how well-equipped you are, if your devices / software are not set correctly you will be in trouble.

My first five rules apply to any computer owner and the second five are in addition for small- or medium-sized enterprises.

Some IT managers would say that a perfectly secured PC is one that is turned-off, and I would agree with this. When you switch a PC on, the probability of losing your data will rise, even when not connected to the Internet, for the simple reason that hardware can fail any time. The hard disk is one of the weakest points of a PC and the possibility of your IDE/ATA hard drive falling apart is much greater than you might imagine. You might also delete a file by mistake. To be sure of not losing anything, you need to have a back-up for your data: DAT, DLT, AIT, CD, DVD, or other media.

Therefore, my rule number one is make a backup for/of your valuable data.

Just 15-20 years ago, the chances of being infected by a virus were rather low and few had access to the Internet, while people were using incompatible operating systems. The main source of contamination was the exchange of diskettes and pirated software. But now that most people use Microsoft Windows, viruses are spreading at the speed of light, and within half a day the entire world can be at risk. Viruses and worms are pieces of code that attach to a file and then replicate, usually arriving as executable files or macros although recently a virus was found in picture file (jpg). Some kinds of virus can be really destructive and having an antivirus program is mandatory and it must be frequently updated, or it is useless.

My rule number two: Install an Anti-virus program and keep it updated.

When you first set up Windows, you have few choices to select what you want on your desktop. By default, Windows will install a lot of unnecessary files, programs and services which cannot be removed by the "add/remove programs" in the control panel. These needless files are potentially unsafe and can be used by hackers. In an office environment, some default programs make no sense: who needs to play with Movie Maker, Games (Freecell, Hearts, Solitaire, etc.), Messenger or the accessibility options (on-screen keyboard, Narrator, etc.)? To harden and speed up your operating system, you should install only what is required. Removing such programs may be not be easy, but you can use a dedicated tool such as nLite by Nui (freeware) or xplite from LitePC. But, be careful to make sure that you do

not remove important files.

My rule number three: Remove all unnecessary files, programs and services.

Updating Windows is now essential. Attackers use security weaknesses to exploit vulnerabilities in some programs. Critical updates are crucial to security, to fix bugs and close unsafe doors to the outside. An easy way to check if your Windows is up to date is to go to Windows Update in Internet Explorer; but if you have many PCs to manage, I would suggest MBSA (Microsoft Baseline Security Analyzer), a free vulnerability assessment tool for the Microsoft platform.

When you are dealing with few PCs, this is not a big problem, but for a large corporation it is not an easy task. Fortunately administrators have several possibilities to update PCs quickly and efficiently using SUS \_ Microsoft Software Update Services (free) \_ or a specialised patch management tool such as Ecora Patch Manager, HFNetChkPro or UpdateEXPERT.

My rule number four: Keep your operating system updated.

When connected to the outside world, your most important device should be a personal firewall. "Don't go out without one." A firewall protects enterprise assets and business transactions by ensuring fast and secure connections with the Internet and between networks. They come in many flavours: software or appliance, single or multiple functions attached such as VPN, antivirus, IDS, IDP, content filtering etc., some manufacturers even propose all-in-one solution (Proventia-G from ISS).

If you are an individual, my first suggestion is: use the firewall included in Windows XP Service Pack 2 (for basic use) or install a freeware/shareware such ZoneAlarm, Kerio Personal Firewall, Sygate Personal firewall, etc. An enterprise should select a firewall adapted to its needs (bandwidth, NAT, authentication, VPN, protection against SYN floods, H.323 based services, malicious code, etc.) However choosing a firewall for an organisation is not an easy task, for the simple reason that very few benchmarks are available and models keep on changing.

My rule number five: Install a firewall and configure it correctly.

Assuming you have a local network with a certain number of PCs, anyone with access to any of these PCs can easily steal valuable data with a simple USB flash drive . In addition, network administrators should control access to PCs to avoid viruses, Trojans and other malicious programs often injected from removable media (pirated games, hacking tools, etc.). To avoid such a loss from the introduction of foreign media, you need to protect your PC's ports such as USB, serial, infrared, Bluetooth, CD player or floppy disk drives, etc. Only the administrator should be able to give the right to access PC's port. Software is available on the market such as DeviceLock from Smartline.

My rule number six: Block all access ports.

Another risk is the access to the motherboard BIOS. The first step should be to set a password to lock it. The first bootable device should always be the hard disk. With access to the BIOS, someone can effortlessly crack your PC's administrator password with a bootable CD filled with some "utilities".

Rule number seven: Set the motherboard's BIOS password.

When connected to a LAN, users should not be permitted to install and run software. With access to the Internet, anyone can download potentially dangerous programs thus jeopardizing the whole LAN. Windows 2000 Server and 2003 Server have a powerful tool to manage user rights, the GPO (Group Policy Objects). With this, you can set up a policy to manage and secure your network. A multitude of rules can be defined: complexity of the password, screensaver, authorised applications to be run, auditing, and you name it.

Because Group Policies can have a tremendous impact on users, any Group Policy implementation should be tested carefully before implementation.

Rule number eight: Set up the Group Policy Objects rules.

Being connected to the web brings a lot of benefits, speedy exchange of mails, plenty of information \_ and also unwelcome content to employees. Risks are wasted time, network exposure to potential dangers and wasted bandwidth. To avoid massive downloads of software, music (mainly MP3) and video files (MPEG, AVI, MP4, WMV, MOV, WMA, etc.) through P2P, HTTP, FTP and email attachments, filtering must be implemented and be able to recognise content.

Rule number nine: Use a content filtering software for HTTP, FTP and SMTP

If you go to some websites and register for some newsletters, updates, etc., the chances that you will receive Spam or unwanted mail are high. Anti-Spam software is becoming a necessity and should be installed to avoid wasted time and unwanted mail.

Rule number ten: Use anti-Spam software.

Above rules are arbitrary, they only reflect what I consider to be important points to secure PCs and networks. In fact the first question to answer is what to protect, how much am I prepared to spend to safeguard my data?

Small and medium enterprises should decide how much freedom to give to their employees. How far should they trust them? The response depends on time and money available and the level of protection desired. Since you cannot have a 100 percent secure network, you have to choose your priorities.

Louis Menthon was IT security manager of a life insurance company in Luxembourg and is now consultant for NetONE.