

Security: Best Practices for Network Security

Best Practices for Network Security

First, it is important to realize that this article is in no way intended to provide a comprehensive, all-inclusive solution to security problems for networks and database servers. This article is meant to serve only as a minimum foundation for setting up security for a network. It is important to always consult a local Microsoft Network Engineer or other certified technician for a full and complete review of any security configuration.

Second, understand that there is no such thing as an absolutely secure system; there are only different levels of security in a network. Time and time again hackers have proved that nothing can be totally secure, but nevertheless it is still important to take a few simple steps toward protecting networks from unwanted access.

A useful analogy for understanding computer security is securing a house. One would not think that simply installing doors in a house would be enough to keep it secure. At the very least, the doors would need locks. Often even simple locks are insufficient, and deadbolts are required for greater security. A greater level of security and protection would include alarm systems that sound an alert and notify the authorities. All these are considered good security practices, but the fact still remains that a determined intruder can smash a window with a hammer in order to gain access.

Now, consider a few misconceptions about network security. First, no Windows ME or Windows 98 systems are secure. They can be accessed by anyone who can gain access to your network, either physically or via the Internet. Both 98 and ME must be behind a firewall. Neither operating system was designed to be secure on an open network. Security is simply not integrated into their basic file systems. Any knowledgeable computer user can gain access to a Windows ME or Windows 98 system in under ten minutes if it is not secured behind a firewall. Second, network access to any computer means that it can be compromised. It only takes a matter of a few hours, perhaps only a few minutes or seconds, for an expert to compromise a improperly secured computer system with nothing more than network access to that system. Finally, direct physical access to a computer is the equivalent of the hammer in the house analogy. Even the most elaborate, robust network security system is of little value if a thief can walk into an office and steal a computer and all the data it contains.

Feeling a little vulnerable? Consider some common, basic level, security vulnerabilities and precautions:

1.) Firewall: If a computer is connected to the Internet, it needs a firewall. A firewall is simply device that controls what services and applications which are allowed to communicate between the Internet and a local network. All network activity and traffic must pass through a specific numbered connection between the computer and the network. These connections are called ports. For example: web pages run on port 80, email runs on port 25, and Microsoft SQL database servers run on 1433 and 1434. Think of a firewall as the wall around a castle, with doors (or ports) that only let certain people (or network traffic) in or out, while preventing unauthorized traffic from passing through. By default, most firewalls have all but port 25 and 80 closed. Most firewalls can be configured to allow or deny access to any given port.

In addition, most users configure their firewall to run Network Address Translation (NAT). NAT is a simple concept that provides minimal protection to computers on a network. Each computer that is connected to the Internet is assigned a unique computer number called an IP address. This number allows other computers and routers to communicate across the Internet without information being lost or given to the wrong computer. NAT hides computers from the outside world by using a network's outside IP number, and then issuing internal private IP

numbers to computers inside the network. These private IP numbers cannot be seen from outside the network, so to outside systems the entire local network will appear to act as a single computer with a single address.

For example, a computer inside the network requests something outside the network, such as a web page on the Internet. This request is sent first to the firewall, which then sends the request out to the Internet. The web server on the Internet receives the request (which now appears to originate from the firewall rather than the local computer), processes it, and sends it back to the firewall. The firewall then sends the request back into the local network and to the appropriate computer. The web server knows nothing about the local computer and local network, as it only communicated with the firewall. Therefore, as far as the Internet is concerned, the local computer does not exist, only the firewall exists. Think of NAT as a guard at the door who relays messages to and from the inside of the fortress, but remains the sole representative of the castle inhabitants, regardless of how many inhabitants there may be.

2.) Controlled Physical Access: Controlling physical access to the computer itself is the second most important aspect of network security, even if a local network is not connected to the Internet, and especially if a computer is running Windows 98 or Windows ME. On a Windows 98 or Windows ME computer, anyone who has direct physical access to that computer will have unlimited access to all the data files on that computer. Usernames and Passwords are of no value on these systems, since the login procedure can be easily circumvented, and even the Built-inscreen saver with a password does not offer any real access protection. Additionally, it is important to remember that computers are relatively small and portable, and can be easily stolen or damaged. Never allow a computer holding sensitive data to be vulnerable to physical theft. Simple, inexpensive measures such as key and chain lock systems can provide powerful deterrents.

3.) Secure Operating Systems: Windows NT, 2000 and XP are considered to be secure operating systems, provided they use the NTFS file system instead of the older, less secure FAT32 file system. Usernames and passwords are mandatory on these operating systems. Access to data, functions, and applications can be limited to specific users, with each user identified by a unique login name and password. When sharing data or resources on one of these systems, it is possible to limit access to only specific users or groups of users. Although it can be very convenient, sharing folders or files to everyone is very insecure, as it allows any computer or user on the network to access those shared files or folders. Passwords should always be at least 7 characters long, and should never be words that appear in a dictionary. Ideally, they should also include numerals and special characters, in addition to containing a mixture of uppercase and lowercase letters. For example the password "blessed" meets the 7 character rule, but is in the dictionary. A password such as "bL@ss&d" would be much more secure because it is not in the dictionary and it includes unusual characters. These measures make this password thousands of times harder to crack than a simple word. However it is important to always remember passwords, since it can be difficult or even impossible to access a system if the password has been forgotten. One trick that is useful in remembering your password is to use simple sentences such as `i_crossed_the_street_today$`. As you can see it is easy to remember, but meets all our criteria for a good password, over 7 characters and unusual characters and because it is ran together, not in the dictionary.

4.) Backups: Regular, carefully planned backups are one of the best, and most important, security measures. Data loss caused by theft, viruses, worms, or hardware failure is always bad, but the damage can be mitigated by having a good, reliable backup system in place. Backups to tape, CD or any removable data can countless hours and dollars in an emergency.

5.) Viruses: Computer viruses are one of the most potentially destructive security attacks. Virus protection programs are an absolute must in any network where computers are accessing the Internet, CDs, floppy disks, or emails. Yes, even email! Email is the number one carrier of viruses. While text-based email cannot carry viruses, attachments and html messages with redirects can. The most common entry point of viruses in networks is an attachment to an email. No matter how secure the network is, if someone receives an email that has an executable attachment (such as a file ending in .exe) that contains a virus, and opens that attachment, the virus will infect the computer. At that point, it is the virus protection software's responsibility to detect the virus, then delete it or place it in quarantine. There are many virus protection software makers on the market both Norton Antivirus Corporate Edition (<http://www.symantec.com/>) and McAfee Security (<http://mcafee.com/>) are ones that are considered industry standards. NOTE: Firewalls are not adequate protection against viruses, since many viruses can masquerade as legitimate programs!

6.) Wireless Access: If an office deploys a wireless networking solution, they should be sure to activate the manufacturer's built-in encryption and security measures. All wireless solutions should utilize some level of encryption. Most utilize a protocol called "Wired Equivalent Privacy" (WEP). The better wireless access points utilize "Temporal Key Integrity Protocol" (TKIP). WEP uses a static encryption key set, where TKIP uses a dynamically assigned encryption key set. The bottom line for most users is that WEP is good enough for current HIPAA security standards (as of 02/02/2003), but TKIP is a much better security solution. Neglecting to use wireless encryption can allow anyone with a laptop or handheld computer and a wireless network card to walk within range start using a network just as if they had plugged into a wired data port in the office.

7.) System Maintenance: Computers and their software are created by fallible humans, and therefore inevitably contain inherent flaws. This is a fact that will never change. Microsoft is trying to stay one step ahead of these flaws with the Windows update site: <http://windowsupdate.microsoft.com/>. This site provides a list of what updates are available for the Windows operating system, and provides an easy way to download and install them. In addition, users who are running Microsoft products such as MSDE and SQL Server may find these two sites helpful <http://www.microsoft.com/security/> and <http://www.microsoft.com/sql/>

In summary, having a firewall in place, using a secure operating system, using complex passwords, limiting physical access, having a comprehensive backup strategy, using virus protection, enabling encryption on wireless solutions, and keeping systems up-to-date with the latest patches and service packs all form the foundation on which to build a secure and reliable network.

Resources on the web that can help you with security issues:

Microsoft's:

TechNet IT Download Resources:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/downloads/itdownloads/default.asp>

The Ten Immutable Laws of Security:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/essays/10imlaws.asp>

Baseline Security Analyzer

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/MBSAhome.asp>

Make your Windows Servers Secure:

<http://www.microsoft.com/technet/security/tools/ChkList/WSrvSec.asp?frame=true>

Security Tools and Checklists:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools.asp>

Non-Microsoft resources

GRC

GRC is a great place to see how visible you are to the internet. Use the "ShieldsUp" program to run an outside audit of your system. Then run "Probe My Ports" to get a better understanding of what ports on your computer are available to the Internet. Free.

<http://grc.com>

GFiLanGuard

Get an idea of what a hacker sees on your network by looking in from the inside or outside. Great tool for finding holes in your security. Free download trial version available.

<http://www.gfi.com/lannetscan/>

Symantec's Online Security Check

This online security check will evaluate your accessibility to the internet and your current virus protection. It is a pro Symantec product, but a good scan. In addition, they also have a free online virus scan.

<http://security.symantec.com/ssc/home.asp>

McAfee's FreeScan

This online tool will scan your computer for Viruses and give you an idea of how to clean them off.

<http://www.mcafee.com/myapps/mfs/default.asp>

PC Magazine's Security Watch

PC Magazine has long been know for its in depth knowledge on computer related issues. Security Watch offers great insight into products and configurations that can better your security.

<http://www.pcmag.com/category2/0,4148,12,00.asp>