

Network Security- By Jeff Lenning, President

Originally Published in "Orange County Lawyer" magazine - December 2002

Overview

A secure computer network is of paramount importance in today's technology climate. Securing your network does not need to be expensive or confusing. Protecting the confidential data that exists on your network is critical for business success. The compromise of confidential client information could result in litigation. In addition, significant business interruptions can occur in the event of data loss. This article discusses strategies to combat the 4 primary threats to your network and the data it contains:

The purpose of Remote Access is to deliver all of the files on your office network to the remote location in our case, home. There are various methods, each with varying degrees of cost, security and performance. The alternatives discussed in this article are:

- Hardware failure
- Human error
- Hackers
- Viruses

Hardware failure

One of the most common causes of data loss on a computer network is hardware failure. Computers are made of many physical components. The failure of a key hardware component could result in data loss. The two primary strategies to protect against hardware failure are:

- Backups
- Hardware Redundancy

Backups

A good backup strategy includes two primary elements:

- Removable media
- Automatic

Removable media

A successful backup strategy will allow you to remove the backup media and take it off site for a period of time (usually overnight). This allows the separation of the computer network and the data backup. Taking the backup media offsite protects it from natural disasters and theft. Good alternatives for removable media are burnable CDs, Zip disks, and tape.

Automatic

For a backup strategy to be reliable, it needs to be automatic. If the backup relies on a human to start the process, a point of failure exists. The backup should occur automatically every night. There are various backup software programs available, including the free backup program included in various Microsoft Windows versions.

Having a good backup is extremely important to help recover from a hardware failure. The second way to protect against hardware failure is to have hardware redundancy.

Hardware redundancy

A good computer motto is "redundancy in all things". Redundancy is a term meaning, "have a backup plan in case something breaks." For example, using dual power supplies on your server, so if one fails, the other will supply power and the computer will stay on. The idea is to have backup hardware components so that in case one breaks, the backup component will turn on and the server will stay up. Another example of hardware redundancy is multiple hard drives. There are various configurations of redundant hard drives called RAID levels, but the simplest example is two mirrored drives. Both of the drives contain the exact same information at all times. In the event one breaks, the other will supply the information to the organization. Some larger companies take redundancy so seriously that they have redundant servers so that if one breaks, the second server will kick in with no interruption in service. Hardware redundancy is critical for servers that contain the information on your network.

Human error/intent

Another threat to your network and data is human error/intent. An example of human error is when an employe accidentally deletes a needed file. An example of human intent is when an upset employee intentionally delete files. There are two primary methods for protecting against human error/intent:

- Backups
- Access rights

Backups

In addition to the backup strategies discussed above, it is important to retain a history of your backup media. Retain backup history allows for the recovery of files that were deleted a few days ago. It is recommended to retain at least a week of backup history, and potentially one backup media for each prior month or quarter.

Access rights

Access rights are set up in the network to allow employees to only see and modify files that they need to see for their particular job function. If an employee does not need to see a file for his/her job role, the employee should not have access to the file. This will help to protect certain files from accidental or intentional deletion.

Hackers

A growing threat to your computer network is the hacker. This threat is becoming more and more significant as companies obtain "always on" internet connections like dsl and cable modem.

There are three primary ways to help keep hackers out of your network:

- Firewall
- Employee education
- Good password policy

It is important to note that given time and determination, a hacker can most likely obtain the information on your computers. The key is to try to make it hard enough that the hacker will move on to easier targets. It is like the saying, "You don't need to run faster than the bear; you just need to run faster than your friend."

Firewall

If you have an "always on" internet connection, you need to have a firewall. A firewall sits between the internet and your network and manages the network traffic. Unless you have a true firewall, you could be exposing your computer network to hackers. There are various hardware and software firewalls available. It is important to note that the dsl/cable "router" that sells at your local computer store for about \$100 is not necessarily a true firewall. These inexpensive boxes typically rely on Network Address Translation (NAT) to buffer you from the internet, and are marketed to home users. Although NAT router is better than nothing, a hacker can bypass them. A true stateful packet inspection firewall is important to place a solid barrier between the internet and your network.

Employee education

Employee education is just as important as a firewall. Hackers often resort to "social engineering" to obtain user names and passwords. For example, they may call an employee and state that they are "Bob from IT" or "Joe from your internet service provider". They will then attempt to persuade the employee to reveal their password. Employees should be informed to never give usernames or passwords over the phone to anyone.

Password policy

A good password policy demands that employees never write their password down next to their computer. In addition, a good password policy requires that passwords are changed periodically and that passwords are complex. Hackers of times will use a "dictionary" of common passwords and all words in an English dictionary to "brute force" their way into the password. A complex password uses a combination of upper and lower case letters, numbers and special characters.

Viruses

A growing threat to your network data is viruses. In the "old" days, viruses were primarily benign and simply annoyed the recipient. However, the new breed of viruses, worms and Trojan horses can create disaster on your network and cause data loss and lost productivity. The two common methods for protecting against virus attacks are:

- Anti-virus software
- Employee education

Anti-virus software

Anti-virus (AV) software should reside on every computer on your network and continually scan each file for the existence of a virus. If a virus is found, the software should either delete or otherwise quarantine the file to prevent the virus from doing any damage. The biggest pitfall in AV software is "definition updates". People incorrectly conclude that since they have AV software they are safe. However, since new viruses come out daily, it is critical that the AV application checks the internet daily to get the latest updates. The next step up in security is to actually force the computer to have the current definitions, which is accomplished through certain hardware devices. This method ensures that all computers on your network have the most current updates. Finally, an email attachment filter should be installed so that key email attachment file types are automatically disabled.

Employee education

Employee education is important in fighting the war against viruses. First and foremost, employees should be instructed to never open a suspicious looking/unexpected email. The simple fact that the email is from someone they know does not indicate that the email is safe. A virus can propagate through email by sending itself to all contacts on the computer.

Conclusion

There are practical steps that should be taken immediately to help protect your network and the data that exist on it. When computer problems arise, lost productivity and frustration result. To keep your business running smoothly, you need to keep your computer network running smoothly. Implementing the strategies mentioned in this article will help. To obtain an idea about the current state of your computer network, take our free online security survey. To request further information or to discuss how to improve the security of your network, feel free to contact us.