



Protecting Your Organization From Viruses

By Mark Bella

In the IT world, it's not uncommon to hear about a new virus outbreak on a regular basis. There are well over 100,000 known computer viruses in the world.¹ In 2005, viruses caused 14.2 billion dollars in damages.² With that being known, it is important to take defensive steps to protect your organization. Unfortunately for a large number of organizations the security measures taken are not enough.

The primary source of viruses originates from the internet. How they enter your network could be one of a number of ways; downloading content, emails, hacking attempts, infected disks. The most common line of defense, and in most cases the only line of defense against viruses, is installing an antivirus agent such, as Symantec Antivirus, on computers. This will scan emails, downloaded files, and operating system files for viruses. Once a virus is detected it will try to clean the file, but if that fails it will quarantine or delete the file. This is a great initial step in securing your organization, however you must be sure to keep your antivirus software and definitions up to date. The antivirus agents are only as good as the virus definitions installed. An antivirus agent with week old virus definitions will not be able to detect the virus, worm or Trojan that arrived in your email inbox this morning.

In some instances, antivirus agents will detect a virus on a computer, but will not be able to clean, delete or quarantine the virus. In these cases, reformatting the computer would be the most practical solution; however this will cause a lot of overhead and headaches. The solution to this problem is to stop viruses from entering your network in the first place by placing a firewall between your network and the internet. A standard firewall will only protect you against hacking attempts. However there are firewalls that perform antivirus scanning on the wire. The antivirus firewalls hold data in a memory buffer, once all the data has been received, it's scanned for viruses and once the file has been scanned, it is passed onto the client. Another benefit with utilizing an antivirus firewall is that it will also scan outbound traffic. This will help identify infected computer on your network so you can take corrective action.

¹ Computer Knowledge: <http://www.cknow.com>

² Computer Economic: <http://www.computereconomics.com>



With software and hardware antivirus protection, keep in mind it's still possible for a virus to slip through and delete, corrupt or modify your files. It is important to backup files on a regular basis. Develop a backup plan for your organization should be top priority. You should backup your files at least one per day. Depending on how critical the data is, you may want to consider incremental backups during the day. It is also important to verify the integrity of your backups on a regular basis. The backup logs may say the backup has been completed, but the data on the tape may be corrupted or un-restorable.

You've probably seen on the news that a new "Windows Security Flaw" is discovered on a regular basis. Microsoft has a security bulletin to identify these flaws and their fixes. It is important to keep up to date on these security flaws and apply all applicable security patches and hot fixes. Many of these patches and hot fixes are to correct security flaws that allow remote execution of code which can be exposed through a specially created webpage that can exploit the flaw and may lead to file corruption, virus downloads or even theft of private data.

Probably the weakest point in any organization's security is their people. It is critical to establish computer policies, which are just basic rules and safe practices, for all people to follow. It is also a good practice to not allow software to be installed without first consulting your IT staff to ensure it is safe and does not contain any hidden viruses or "Trojan horses."

It is important develop an approach that accounts for all aspects of securing your network and computers from unwelcome attacks. Focusing on just one of the mentioned security measures is not enough. A sound strategy incorporates many facets and layers security measure together which result in a model that is several time more effective in protecting your network.