

Network Protection for Design Professionals

Virus Controls and Filtering

Background:

Anti-Virus — anti-virus software packages look for patterns in files or memory that indicate the possible presence of a known virus. Anti-virus packages know what to look for through the use of virus profiles or “signatures” provided by the vendor. Since new viruses are discovered every day it is important to have the latest virus profiles installed. Without this protection, viruses are free to infect your systems. Viruses may cause a variety of problems such as loss or damage to information residing on your network, network interruption and inability of customers to access your system. Liability may be incurred if weaknesses of your security measures allow the systems of third parties to be infected. It has also become commonplace that viruses carry a spyware payload. See further description below.

Spyware — refers to a category of software that, when installed on a computer, collects personal information about a user without their informed consent. Spyware

may be unknowingly downloaded by users when packaged in a Trojan Horse or systems may be infected by viruses that include a spyware payload. There are significant privacy liability implications due to the information that is being harvested and sent to a third party without the user’s consent.

Controls on shared drives and folders — a network share is a location on a network allowing multiple users on that network to have a centralized space on which to store files. Unprotected Windows networking shares can be exploited by intruders in an automated way to place tools on large numbers of Windows-based computers attached to the Internet. Unprotected shares can allow Distributed Denial of Service attacks to occur and are also leveraged to propagate viruses and worms both internally to a network and to other networks. There is great potential for the emergence of other intruder tools that leverage unprotected Windows networking shares on a widespread basis.

How to implement appropriate controls:

Anti-virus

- Install anti-virus software on all systems.
- Implement a process to keep anti-virus programs up to date, utilizing automatic update of virus signatures if possible.
- Filter e-mail attachments and downloads to reject files with the following extensions: .exe, .vbs, .bat, .pif, .scr.
- Disable unneeded services and ports including: FTP service, telnet.
- Train employees not to open e-mail attachments unless they are expected and from a known and trusted source.
- Execute anti-virus scans on all e-mail attachments, files and downloads before the file is opened.

The links below provide additional anti-virus resources:

- **US CERT Computer Virus Resource**, http://www.us-cert.gov/reading_room/virus.html
- **ISCA Lab**, [http://www.icsalabs.com/icsa/product.php?tid=dfgdf\\$gdhkkjk-kkkk](http://www.icsalabs.com/icsa/product.php?tid=dfgdf$gdhkkjk-kkkk)

Controls on shared drives & folders

If sharing of directories and files over your network is not essential, file sharing should be disabled. An alternative would be to create a dedicated directory for file sharing, and move or copy files to that directory for sharing. All network shares should be password protected and restricted to read-only access when possible.

Network Protection for Design Professionals

Removal of spyware

- At minimum, run a monthly full scan with anti-virus software on all computers on your network. Anti-virus software may find and remove spyware during a scan that it does not detect during real time monitoring.
- Run a legitimate product specifically designed to remove spyware.

A list of popular products can be found at the following link:

- **ICSA Labs**, [http://www.icsalabs.com/icsa/topic.php?tid=962c\\$b7edc94e-dd775595\\$1d7a-48391663](http://www.icsalabs.com/icsa/topic.php?tid=962c$b7edc94e-dd775595$1d7a-48391663)

Vendor Neutral Threat Notification

It is important to utilize a vendor neutral source of vulnerability and threat information in addition to other information that may be received. This assures that timely, non-biased threat notification is available for the coordination of appropriate defenses.

Use one of the links below to subscribe to a source of vendor neutral threat information:

- **CERT National Cyber Alert System**, <http://www.us-cert.gov/cas/signup.html>
- **SANS Institute @RISK: The Consensus Security Alert**,
<http://www.sans.org/newsletters/risk/?portal=6ea651380cdb76a250c69e382baf5c61>

References:

- <http://www.us-cert.gov/cas/tips/ST04-016.html>
- http://www.us-cert.gov/reading_room/home-network-security/#III-B-5
- http://www.us-cert.gov/reading_room/virus.html

