Monthly Cyber Security Tips

NEWSLETTER

AUGUST 2008 Volume 3, Issue 8

Firewalls

From the Desk of Darrell Davis

What is a firewall and why should I use one?

A firewall is a software program or hardware device that filters the inbound and outbound traffic between your network or computer and the Internet. Firewalls add a layer of protection by blocking unauthorized and potentially dangerous data from entering your computer or network. Firewalls are especially critical for users who have an “always on” connection to the Internet.

Some users may think that data residing on their computer is not valuable and therefore a firewall is not necessary. However, even small pieces of information can be obtained by the hacker and used to steal identities and other personal data. In addition, hackers may be interested in taking over your computer to store illegal materials or launch other attacks that can leave a trail back to your computer. Once a hacker gets access to your computer, the intruder may have access to resources and data stored on your machine.

What does a firewall protect me from?

Firewalls can help protect your data and computer by blocking the following:

- unsolicited traffic/malware from coming into your computer or network
- traffic from known malicious computers
- specific traffic you don’t want leaving your computer or network
- programs, protocols and ports that you specify
- attempts to access or attack your computer

Firewalls can also log activity, and these logs should be reviewed periodically to identify any anomalous or unexpected activity.

What type of firewall should I use?

There are two types of firewalls: hardware and software. A hardware firewall is usually an external device that sits between your computer and your connection to the Internet. A software firewall (also known as a personal firewall) runs directly on your computer. This firewall is the most common type for home users.

The selection of a firewall is dependent on what is being protected. The value of the assets,

the complexity of the computers or networks, and their usage of the Internet will dictate the type and size of firewall that should be used.

Make sure you have a firewall--selected based on your business or personal needs--and that it is enabled.

Before enabling a firewall, read the documentation carefully to ensure proper configuration. A properly configured firewall can save you hours of recovery or rebuilding of data.

Below are some areas for consideration when installing a firewall:

- allow only the traffic that you need
- enable the "automatic update" feature if one exists and also periodically check the firewall vendor's website for the latest software updates
- enable the logging feature and review the logs regularly
- change the default "administrator" account (if available) and password
- disable the remote management option (if available)

A firewall is a very valuable tool to protect your data and your computers, but it must be selected, installed, configured, monitored, and maintained effectively to do its job. It's also important to note that although firewalls can block intruders, viruses or unwanted traffic from getting into your computer, using a firewall is not a complete solution to security. Firewalls should be used along with anti-virus, anti-spyware, and anti-spam software, as part of a defense-in-depth strategy for protecting your computer from various forms of malware (viruses, worms, trojans, etc.), hackers, and others who want your data or your computer for illegal or malicious purposes.

Remember: Cyber Security is Your Responsibility. Always apply safe cyber security practices to protect the data on your computer or network.

References
To learn more about firewalls, please visit the following sites:

MS-ISAC - Beginners Guide to Firewalls
http://www.cscic.state.ny.us/localgov/#download

US-CERT
http://www.us-cert.gov/cas/tips/ST04-004.html

How Stuff Works - Firewalls
http://computer.howstuffworks.com/firewall.htm

Firewalls for Dummies
http://www.dummies.com/WileyCDA/DummiesTitle/Firewalls-For-Dummies-2nd-Edition.productCd-0764540483.html

Resources – For previous issues of the Monthly Cyber Security Tips Newsletter go to:
http://www.msisac.org/awareness/news/

Organizations have permission--and in fact are encouraged--to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture.

.

Brought to you by:
MS-ISAC *http://www.msisac.org*