Why a Dedicated Firewall Would Be Beneficial for Your Business

Regardless of the size of your business, odds are you have confidential information, such as trade secrets, financial records, or client information, that you need to keep secure from potential data theft. The potentially staggering financial losses connected with stolen data and comprised network security can cause serious problems for a business. These losses can be avoided by installing a dedicated hardware firewall on your network.

Far too many business either have no firewall or opt to use software-based firewalls, such as those built into common antivirus software packages or included in their PC operating system. While software firewalls may provide some limited protection on a computer-by-computer basis, they do not provide the kind of robust, whole-network that modern business need and can be far more vulnerable to threats than a hardware-based firewall solution.

A firewall is your first line of defense against unauthorized intrusion into your business network. As the name implies, it acts as a literal 'firewall' that insulates and separates your internal computers and computer network from the internet. The purpose of the firewall is to monitor any inbound traffic into your network for suspicious data that may be a sign of a hacker trying to get into your network and to block this traffic. A properly configured firewall can also monitor outbound traffic from within your network to the outside world and look for outbound data traffic that could be indicative of a virus infection on your network.

The most important role of a firewall, however, is to keep your internal network safely secured away from the internet, and to only allow very specific types of data traffic as determined by the firewall administrator – such as HTTP, for web browsing, or FTP, for file transfers – on very specific communications ports to access computers within your network. A firewall can also limit what specific ports individual computers on your network can access for specific types of outbound or inbound data traffic, and what websites employees are allowed to visit. Limited what web sites employees are allowed to access can be invaluable, since many business virus infections and data incursions are caused by employees browsing to questionable web sites.

High speed data is a vital part of modern business. However, using this resource without properly securing your business against potential security threats is a disaster in the making.

Contact us if you need further information about firewalls or other options to secure your business from potential data loss.