

Small Business Guide to Network Security

There's good news and bad news. The good news: dropping costs in recent years for broadband Internet, networking technology and Web applications have enabled small businesses to implement technology solutions that in the past were only available to big business. Bad news: use of this technology creates network security vulnerabilities equal to those of large companies and unfortunately, small businesses generally have fewer resources with which to defend themselves against these threats, due to limited information technology (IT) budgets and staffing.

For many companies and security vendors, the answer to all security questions is a firewall, but a firewall is designed to address only one part of the problem. A multi-faceted, layered approach works best. Firewalls were the bulk of a security strategy when companies were basically trying to protect just a local area network (LAN). But now, the landscape has become much more complicated.

The tips listed below are organized according to layers of security and are designed to be a guide to help small businesses take the requisite precautions to protect their network. It is not a replacement for an IT security audit performed by a qualified consultant, but these tips will get a small business well on their way to protecting their IT infrastructure.

Physical Security

This layer of security involves physical access to the network components. It includes servers, desktops, backup media, switches and routers.

- Keep servers and network equipment in a locked room with access given only to authorized personnel
- Secure equipment to desks or other fixed objects
- Store documentation and media securely and dispose of properly
- Use redundant equipment on servers, specifically disk drives and power supplies
- Store servers and uninterruptible power supplies (UPSs) on raised platforms or racks to protect from water damage
- Protect equipment from heat and humidity
- Use UPSs to protect servers, network hubs, switches and desktops from power spikes and sags as well as data corruption due to power failure

Perimeter/Network Security

This layer of security involves threats through remote connections to the network, including the Internet and phone lines. These threats can be numerous due to the vast nature of the Internet.

- Deploy a firewall that blocks all incoming and outgoing traffic unless specifically allowed
- Use personal firewall software on systems with dial-up Internet access
- Utilize dial-back security for dial-up connections
- Require secure authentication and encryption for VPN remote access and make sure VPN user has updated anti-virus and does no peer-to-peer file sharing like Kaaza
- Scan Internet traffic for viruses before it reaches the desktops
- Use a VPN in conjunction with a minimum of 128-bit WEP for security with wireless networking
- Remove and prohibit use of peer-to-peer software such as Napster or Kaaza or any other non-business applications, which can circumvent firewalls and other layers of security
- Log all remote access connections, both successful and failed, for the firewall, Web server and remote access
- Review the logs on a regular basis and look for unauthorized activity
- Document and know your network

creating innovative it solutions



Host Security/Operating System Security

A host is any device on the network, including servers, desktops, printers and scanners.

- Use only secure operating systems such as Linux, Microsoft Windows NT 4.0, 2000 or XP
- Require and enforce passwords that include alphanumeric combinations of characters
- Remove default or blank passwords
- Require password changes at regular intervals and do not allow reuse
- Configure account lockout parameters to protect from password guessing
- Remove inactive accounts
- Remove unneeded services and applications
- Install and document servers patches manually
- Have Windows desktops users install critical updates on a regular basis using the Windows update Web site at <http://windowsupdate.microsoft.com>
- Configure automatic anti-virus software updates on both servers and desktops
- Do not allow end-users to disable virus protection
- Train employees never to open macros or attachments or to download files from unknown or untrusted sources and to report virus detection immediately to minimize damage
- Perform full server backups on a daily basis to eliminate the confusion often associated with incremental backup strategies
- Verify backups are working and test the restore procedures
- Store backup media at a secure, offsite location

Application Security

The application layer concerns the security of the applications that you use on the network. They require much of the same maintenance as do operating systems to reduce vulnerabilities. Additionally, many end-user errors occur at this level, making accidents or misuse the primary vulnerabilities.

- Use application authentication when available with passwords that are different from the network passwords
- Maintain licensed software – unlicensed software can affect both availability and integrity of resources
- Patch applications as necessary
- Train employees in security policies and what to do if they suspect a security threat
- Train network administrators sufficiently and allow them time to maintain security or outsource this to a qualified consultant
- Enforce policies that electronic communication is not considered private and use of Internet or e-mail for illicit, illegal or non-business activities is prohibited

Data Security

This layer protects the integrity, confidentiality and availability of the data. Often, this layer of security is not implemented, but this critical component will protect from inside threats.

- Give users no more privileges than necessary to protect from vulnerabilities such as accidental file deletion
- Implement both share and file/folder permission
- Use encryption for highly sensitive data, especially on portable computers to protect their data in case of theft
- Enforce a policy forbidding distribution of information outside the company without consent
- Train employees in guidelines for proper disposal of hard-copied information

creating innovative it solutions



Security is a dynamic problem with new security threats presenting themselves frequently. The small business network is exposed to many of the same threats as large companies, and the business must be able to protect itself with limited resources. It is critical to implement a security system that is adaptable and easy to manage. Through a multi-layered security structure, a business can defend its network from the majority of threats by focusing on the most important vulnerabilities and then reviewing the security plan and making adjustments as necessary.

creating innovative it solutions