Vol. 5 No. 1
January 2013

BUSINESS insights

Four best practices for LAN/WAN security

Your business uses a Local Area Network (LAN) or Wide Area Network (WAN) to send voice and data to and from employees, clients, partners, vendors and others. This exchange can take place within a single facility or between multiple locations across the country.

Whichever type of network you use, it's vital to keep your business data and communications secure. That's why you should take every step possible to protect those exchanges from theft, fraud and other threats.

In addition to the traditional firewall, virus protection, malware blockers and other types of software or hardware necessary for network security, here are four best practices you'll want to follow that further protect your network and the information that travels across it.

1. Keep servers and application patches up to date.

Failing to add or delaying the addition of patches to network servers or applications can disrupt its operation. Here is the process your business should follow to prevent any potential problems:

Automate the monitoring of the patch status of all your applications. Implementing an automated solution that monitors your network patch status and notifies you when patches are available saves you time and helps keep your LAN/WAN safe. The alternative is to do this monitoring manually. That is, to mark your calendar with periodic reminders to check the respective websites for updates on each of the server systems and applications you use.

Backup your data before installing patches. It's possible for some patches to conflict with your system and cause operational problems. Keeping full up-to-date backups of your system and applications ensures you can restore your data if a patch causes conflicts.

2. Control what files can be shared.

When the individual computers on your system have file and printer sharing activated, files can be copied directly between computers within a business. While this is convenient and helps boost collaboration and productivity, it's important to take care when selecting which folders should be shared.

Folders being shared between workstations are vulnerable to network-aware worms and viruses that can spread from machine to machine. Therefore, it's critical that file sharing never include a root folder, program folders, or operating system folders. Only those folders that contain data files should be shared.

(continue pg. 2)

IDEACOM NETWORK
1-866-IDEACOM
(433-2266)
www.ideacom.org

3. Implement a strong password policy.

Passwords let you control who does and does not have access to your data. Using them is still one of the best ways to protect resources shared on a network. Passwords allow you to limit access to users with a valid user name and password combination. That's why it's important that your business create a strong password policy.

Keep these factors in mind when you formulate your policy:

- Create passwords that are appropriate to the asset being protected. A good rule of thumb for accounts is a minimum of 14 characters using a phrase the user can remember such as "redpicturebicycle."
- Require that passwords be changed on a periodic schedule, such as monthly.
- Educate workers to never leave passwords anywhere visitors or others can see them, such as on a sticky note stuck to a monitor.
- Restrict access to confidential data to working hours only.
- Disable an individual's access to confidential data immediately if that person is terminated.

4. Educate employees on the dangers of using unsecured networks.

The portable nature of laptops leads them to often be connected to the Internet in a multitude of environments. This can include the homes of employees or on public Wi-Fi networks -- like coffee shops, airports and hotels -- that bypass the safeguards you have implemented on your business network.

It's important to educate employees not to trust public networks. Employees should turn off file sharing and turn on personal firewalls when connecting company laptops to public networks. They should be aware that these networks may expose company data to anyone else connected to the same network. Passwords or PINs entered for accounts may be intercepted and/or recorded. Many of these same issues apply to using smartphones, tablets or other mobile devices.

Being aware of the threats and following the guidelines above should help provide a reasonable level of safety for your business LAN or WAN. It's the best way to protect your business and its bottom line.

IDEACOM NETWORK
1-866-IDEACOM
(433-2266)
www.ideacom.org