

Internet Security Issues & Solutions for Small and Medium Networks



***m*elsernet**
making networks work

Melsernet, Inc. • 310 N. Alabama, Ste. B100 • Indianapolis • IN 46204
317.624.1621 • www.melsernet.com



Is Your Network Secure? ... Be Afraid, Be Very Afraid

OVERVIEW

With the growing availability of affordable broadband services such as DSL and cable, your Internet access becomes even more essential to your business. According to the International Data Corporation (IDC), there are currently more than 700,000 small businesses in the U.S with a broadband Internet connection. As small businesses shift from dial-up to **always-on** broadband Internet connections, their networks become more vulnerable to Internet hackers. A single attack can be devastating with all your valuable data wiped out, confidential information stolen or corrupted and your entire network made inoperable.

WHAT ARE THE SECURITY THREATS?

Security is the soft white underbelly of broadband Internet service and the threats are real. How pervasive are security threats on the Internet?

- The Computer Crime and Security Survey published by the FBI and Computer Security Institute found that 71% of all companies reported being attacked by independent external hackers in the last 12 months.
- A Gartner Group survey shows more than over 50% of small and midsize enterprises (SMEs) using the Internet will be hit by hackers.
- According to IDC, the average new DSL connection experiences three attempted “hacks” in the first 48 hours.



Here are the most common types of Internet security threats your business faces.

- 1. Unauthorized Access to Your network.** Hackers may use a variety of readily available “hacker’s helper” tools to break into the network. Once in, the hacker has control of your computer and access to your confidential data.
- 2. Denial of Service (DoS) Attacks.** DoS attacks aim not to steal information, but to disable a device or network so users no longer have access to network resources. Even if your network is not being attacked, it can be used as an unwitting ally in Denial of Service attacks on other networks. So, in addition to protecting your own LAN from attacks, you need to prevent your LAN computers from being compromised and used in attacks on others. DoS attacks are also known as Ping of Death, SYN Flood, LAND Attack and Smurf Attack

3. **Viruses.** Once on your LAN computers, viruses can damage or cause computer crashes. Viruses can also be used as delivery mechanisms for hacking tools, putting the security of the organization in doubt, even if a firewall is installed.

4. **Offensive Content.** Inappropriate Internet content can create an uncomfortable work environment and cause potential legal problems for your business. Not to mention the decrease in employee productivity.


"A 2002 FBI study reported that **78%** of surveyed companies detected employee abuse of Internet privileges, such as downloading pornography or pirated software."


Computerworld 2003

5. **Capture of Private Data Going over the Internet.** As your private data moves over the Internet, hackers using programs called packet sniffers can capture your data as it passes from your network over the Internet and convert it into a readable format. The source and destination users of this information never even know that their confidential information has been tapped.


MELSERNET SOLUTION


Melsernet Internet security products and services provide a comprehensive, integrated security solution that can be tailored to fit the needs of small and medium size businesses. Our core security technologies include firewall, VPN, network anti-virus, content filtering and security management. The good news is that these core security technologies are affordable and will help make your security decision-making easier.

 **Firewall.** No, this is not a 7ft tall by 7ft wide brick wall on fire. Firewalls are a necessary security appliances for every businesses connected to the Internet. In addition, not all firewalls are created equals. Many self-proclaimed "firewalls" are nothing more than "NAT boxes", easily bypassed by "IP spoofing" and lacking the necessary logging and reporting features of firewalls. Make sure that a trusted third party such as the ICSA certifies the security product claiming to be a firewall.

 **Virus Protection.** Virus protection can be accomplished in multiple ways. You can protect against viruses at the desktop or by implementing a gateway that scans emails coming into the network before they reach the desktop. To that, you can add policies to enforce the update of the anti-virus definitions



 **Content Filtering.** Without content filtering, your LAN users have unlimited access to all Internet resources, appropriate and inappropriate, benign and dangerous. There are different methods to create and enforce Internet access policies to block offensive material. You can use Text Screening, where you block sites based on keyword or Allow only Lists, where you block everything and allow certain websites related to your business or use the most common method, URL Blocking, by subscribing to a third-party filtering organization that searches the net and generates a database for all objectionable web sites based on many categories. Third-party vendor are such as CyberNOT, N2H2, Websense and SurfPatrol.

 **Virtual Private Network (VPN).** Today's business environment requires real-time collaboration among geographically dispersed people and offices. According to IDC, the number of mobile workers in the U.S. will increase by 12.7 million between 2001 and 2006, from 92 million to 105 million. In contrast, the number of workers who are not mobile will actually decline by 2 million through 2006, down to 53.8 million. A VPN enables your organization to establish secure communications with remote offices and telecommuters in a manner that is transparent to end-users.

"By the end of 2006 roughly two-thirds (66.0%) of U.S. workers will be mobile workers."

IDC, June 2002

BOTTOM LINE

The bottom line is your business needs to incorporate security into any Internet service implementation. You need to protect your business from Hackers attacks, virus and worms infections and maintain your data secure while telecommuters connect to the office network. There are many factors to consider when purchasing a network security solution for your organization. Melsernet, Inc. with its strategic alliance with Sonicwall offers very affordable integrated security solutions for small and medium size enterprises. To make a better and easier decision about your Internet security, do not hesitate to call Melsernet.

Summarized from *Security Issues and Solutions for Small Business: A White Paper* by SonicWALL, Inc. 2003.

