



Leveraging The World Wide Web

Today's corporate networks have become the intense focus of security management. More networks are connected to the Internet and more businesses depend on the Web for applications such as E-Mail, B2B, and E-Commerce. So how do managers secure company assets from thousands of malevolent products and leverage the World Wide Web?

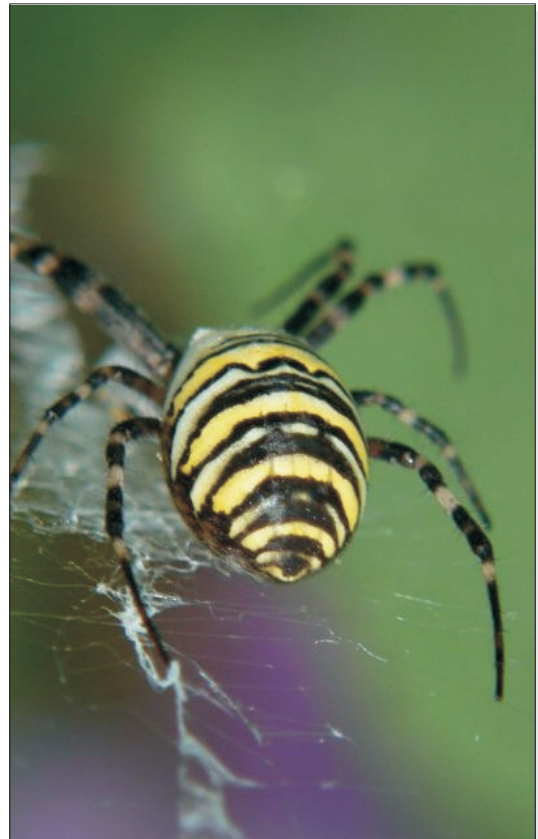
Companies that have sensitive information about their clients, such as social security numbers, health records or driver's license numbers need to be especially careful. Malware, or malignant software, is sometimes the front end of an attacker's offensive. Malware is often used to infect computers and install backdoor agents in order to gain access privileges to systems that are behind corporate firewalls.

Trojan horses, or programs that appear to do one thing but actually have an ulterior motive, can come in the form of download software disguised as a screen saver, an on-line game or even an E-mail greeting card. These programs often execute their primary role by providing the user with a usable piece of software in order to help disguise their real motive: to deposit a dropper (a malicious piece of code) designed to give attackers access to the infected system and its connected network.

Today, router based firewalls are common among interconnected networks but unfortunately they do not offer nearly enough protection. Firewalls stop uninvited, unauthorized traffic from entering the LAN. However, in many cases, LAN users voluntarily (or inadvertently) download software with Malware and install it, so Malware completely bypasses the firewall.

In addition, viruses and Trojan horses often use exploits in the operating system or in the browser to download and install malicious code on computers while users are browsing or viewing E-Mail. This means that you can get Malware simply by visiting a malicious Web page! The best defense against these types of security breaches is an Internet Security Appliance

The home consumer market is extremely competitive and price sensitive. Manufacturers strive to undercut prices, often at the expense of advanced features and security. Yet many businesses purchase consumer or home grade products for use in their corporate networks. Robust business class products, such as Internet Security Appliances are typically not found in stock at your local office supply or electronics retailer. So unfortunately, many businesses do not make use of this technology.





Falcon I.T. Services

Comprehensive Solutions for Small Businesses

← continued from previous page

Internet Security Appliances- Internet Security Appliances combine several types of technologies into a single manageable device. Typical Internet Security Appliances have the following features:

Routing and Firewall- Just like the routers commonly shipped by ISP providers, Internet Security Appliances have built in firewalls and can route local and Internet traffic. They generally have more robust firewalls than most commonly sold routers.

Gateway Filter - Common firewall routers allow approved traffic in and out of your LAN and leave virus scanning, spam control and content filtering up to the software that is installed on each individual's computer. This is the equivalent of letting your children baby sit themselves. Gateway filters on the other hand, monitor all traffic that goes in and out of the LAN. The Internet Security Appliance sits between your LAN and the Internet. Any traffic that flows between the two networks will have to travel through the Security Appliance's Gateway filter. The Gateway filter looks at each packet (each individual piece of data) and scans it for viruses, spam and malware. It also monitors URL requests (requests to view a Web site) and compares them to a database of approved and blocked sites. The sites list is a listing of categories such as Adult, Gaming, Gambling, Crime, Web Mail, Chat, etc. It is a comprehensive list of known sites whose content matches specific categories. The Gateway filter then allows or restricts access to Web sites based on the category list. The category list is customized based on a companies' specific surfing policy. Some companies may want to prevent access to all non-business related sites while other may want to restrict access only sites that may be deemed inappropriate by company managers.

Intrusion Detection – Most good security appliances offer intrusion detection systems. The different types vary by appliance. Most offer E-mail notification against known types of attacks such as DOS (Denial of Service) and can monitor ports for suspicious activity. More advanced systems look for signatures or anomalies in the data flow. Anomalies can include incomplete packets, oversized packets and even data files being transferred during odds business hours. This can safeguard your company against data theft both from outside intruders as well as from insiders.

In conclusion, Internet Security Appliances have become affordable to the point that small businesses should seriously consider such a device as part of their security policy. As large corporate networks become more bulletproof, hackers will inevitable look towards small business that they see as vulnerable. Many small businesses store valuable information on their servers. Whether this information contains personal information about their clients or whether it's proprietary architectural drawings, data theft can cause great discomfort, monetary loss and bad publicity. Adequate network protection is a key element to providing your business and your clients with a smooth and safe operation.



The IBM Business Partner emblem is a trademark of International Business Machines Corporation in the United States, other countries, or both. All other trademarks or registered trademarks are property of their respective owners.

(C) 2006 Falcon I.T. Services
2233 Calais Drive Suite 55A
Miami Beach, FL 33141
(305) 910-4010
<http://www.falconits.com>