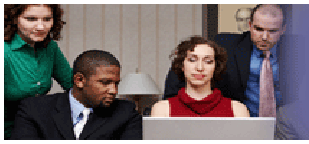
Small and Medium Businesses

The Threat Landscape and the Plan of Action

A study by MicroWorld Technologies



The Threat Scenario

The Small and Medium Businesses contribute to around 68% of the world economy while making up for 80% of the employment. The security needs, issues and priorities of SMBs are different in many ways from that of large Business Houses.

While big enterprises have a well defined security mechanism in place with dedicated personnel to look after it, in most SMBs the scenario is lesser organized, short-staffed and under equipped. They have a small number of IT staff who manages to give only a portion of their time towards the security aspect.

Another major concern is the lack of user awareness owing to a significant presence of under experienced, part-time employees. A recent study by MicroWorld Technologies showed that security awareness is 45% lesser among staffs of smaller businesses in comparison with large enterprises.

One knows small businesses work on stringent standards of Service and Product Delivery models adhering to tight deadlines, as client demands are always on the higher side. Business Continuity is a vital factor for Mid-size organizations in retaining the clientele and fostering relationships. Security breaches and Virus infections in the internal network of organizations can be quite detrimental for Business Continuity as they can bring down the entire network of an organization in a matter of few hours.

Let’s examine these threats in detail.

Virus, Trojan, Riskware and more

Virus

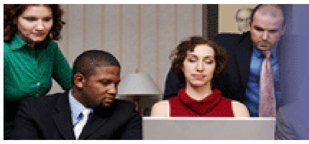
A typical computer Virus is a malicious program that destroys and alters files and folders, while replicating on its own. It usually attaches or inserts itself into an executable file or the boot sector of a disk.

Network Worms

This Malware spreads via P2P File Sharing, LAN, WAN and over the Internet using file sharing programs like Kazaa. A worm wriggling into a vulnerable computer of a large network will send requests to all other machines in order to propagate it.

Trojan

A Trojan refers to a program or a file that may look harmless otherwise, but carries a malicious component in it. Regular Trojans do not replicate on their own, but can be highly destructive, harm applications and threaten your Data Integrity. A MicroWorld study in September 2006 found that 31% of malware caught in SMBs belong to different Trojan families.



Trojan Downloaders
This breed downloads other Viruses, Worms and Trojans into the victim's machine from the Internet. Often they turn off the AntiVirus and Firewall in the system before bringing in new malware!

Trojan Clickers
Trojan Clickers redirect victim's machines to specific websites or other resources on the Internet. They make this possible by tampering with Windows HOSTS file to reroute regular web requests towards websites *they* wish. Trojan Clickers are widely used in increasing the hit-count of specific websites or for launching Denial of Service (DOS) attacks.

Pharming Trojans
This breed is similar to Trojan Clickers and is used in a dangerous attack called 'Pharming'. When an employee from your company's Finance Department accesses the website of the official bank to do a business transaction, he could unwittingly open a spoof website created by scamsters, where he gives away confidential financial information. They do this by making changes in the DNS settings.

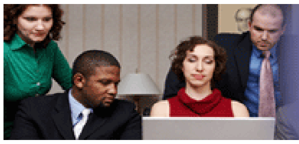
Keyloggers
Keyloggers remain silent in a compromised computer and capture usernames and passwords when a user logs on to the websites of Financial Institutions, Banks and Credit Card Companies. The Information thus stolen is mailed to the author of the Malware. Some of the more evolved ones can take screenshots and capture mouse clicks too. This malicious code is a core component in Password Stealing Trojans.

Keyloggers can pose a dangerous threat to the Data Integrity of SMBs. If they manage to steal the email ID and password of a senior executive, all of his or her mail communication can be spied on, day in and day out.

Backdoor
This Malware is hooked into the victim's system by an intruder, in order to gain Access and Control of it. IRC (Internet Relay Chat) channels are widely used by Backdoors to connect to the attacker and take orders from the criminal sitting in his far away hideout, perhaps in the mountainside Russia! Using the Backdoors, the attacker can operate a compromised computer like his own desktop and execute commands.

Rootkit
A Rootkit is used by malicious programs to hide running processes, files or system data, so that Security Applications do not detect their presence in the computer. They modify parts of the Operating System, install themselves as drivers or kernel modules in order to achieve deep penetration in the computer. It's the favored hiding mechanism for many recent Backdoors and Trojans.

Spyware
Spyware is a risky, malicious program typically bundled as a hidden part of freeware or shareware programs, downloaded from the Internet. It spies on user activities on



computers and sends that information over the Internet to the Malware author.

Spyware eats up system memory, damages its functioning, sneaks into sensitive, Personal Financial Information like Credit Card numbers and passwords.

Adware

Adwares are nasty software programs that pester your computer screens with countless pop-up advertisements. Often they push you to the limits in their attempts to make you visit certain websites, buy tacky products online or join scam services. They can cause system crashing and rob your computing resources and bandwidth, all the while being a perpetual nuisance as well.

Spam and Phishing Menace

Wading through the clutter of Spam is one of the biggest challenges faced by employees of SMBs on a daily basis. Accidentally deleting important and legitimate mails in that process is another issue. Bandwidth issues, Storage Concerns, Loss of Productive hours and Distribution of Malware are a slew of other concerns for organizations, stemming out of Spam mails.

Mail addresses posted on the web and Chat Services are quickly harvested by spammers using an array of techniques to send large numbers of unsolicited emails to those addresses.

Categories of Spam

A research by MicroWorld Labs in July 2006 revealed that the total number of worldwide spam mails per day stands at a staggering 25 billion. MicroWorld categorizes present day spam into segments given below along with their respective shares in the total.

Category	Percentage in Total
Adult Content	23%
Consumer Products	20%,
Health	16%
Finance	14%
IT and Internet	11%
Phishing	6%
Education and Training	3%
Others	7%

60 billion US Dollars is what global business houses lost by way of dent in productivity and wastage of technology last year as a direct and immediate impact of

spam, while its second and third levels of ramifications on the economy could be much deeper and wider.

Port Scanning for Network Hacking

Port Scanning is the most popular searching technique used by attackers to identify vulnerable systems and services in a network. Many services work with TCP and UDP ports and there are as many as 6000 ports currently used in networking.

In Port Scan an attacker sends messages to targeted ports and based on the response it generates, probes deeper for vulnerabilities. TCP ports are targeted the most as they are connection oriented and normally give immediate response to the Intruder.

Some methodologies used in Port Scan are given below.

SOCKS Port Probe

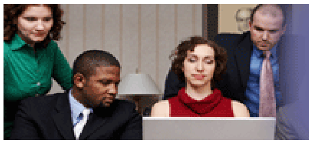
SOCKS is used in a network to facilitate sharing of Internet connection among multiple systems. There's a good possibility for erroneous configuration of some of these ports by some users, creating arbitrary sources and destinations. This helps a cyber criminal to hide his location and access the Internet through the victim's machine.

Stealth Scan

Normal Port Scanning is done with the help of a series of packets rapidly fired at the host. But 'very slow scanning' can be used as a stealth technique to avoid detection. Another such method is called Inverse Mapping, where the attacker finds all hosts in the system by employing "host unreachable" ICMP- messages.

Fragmented Packet Port Scan

This is done by breaking a TCP header into several IP fragments. Many firewalls can be tricked by this technique as they normally try to match the whole TCP header to identify an attempt of intrusion.



How to protect your Information Systems?

The ideal solution plan for Mid-size firms looking to protect their Information Systems from a variety threats mentioned so far would be to rely on comprehensive AntiVirus, AntiSpam and Content Security Solutions with a Central Management Console. A powerful Network Firewall is also a necessity to defend against intrusions. The system or systems should scan all HTTP and FTP traffic for malicious code, block spam and phishing and provide policy based Access Control for the entire organization.

Let's first see what all capabilities an **AntiVirus, AntiSpam and Content Security** solution should have.

Real-Time Malware Scanning with the Earliest Detection of new threats

First things first. The prime job of an AntiVirus is to detect and block all sorts of malware. It should check e-mails and websites in real-time for Viruses, Worms, Trojans, Spyware, Adware, Keyloggers, Backdoors, Rootkits and more. It must have the fastest and earliest updating database for detection and removal of all kinds of Malware including latest exploits targeting vulnerabilities in Operating Systems and other Software Applications.

Behavioral and Intentional Analysis

The system should employ a highly sophisticated Behavior and Intention Analysis method to identify unknown Viruses and Worms. This means the AntiVirus will proactively block even that malicious code, whose signature is not present in the AntiVirus Database.

Integrated Security Policy Enforcement

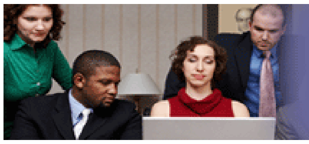
The Management Console of the software must enable the network administrator to view and access the entire network architecture, including activities at different workstations. Features should allow the administrator to distribute new updates across the network. Options are required to block Active X controls and stop exploit codes and Trojan Droppers targeting browser vulnerabilities. The software should make sure that no unwanted program is installed in your computer in deceptive ways.

Remote Web Administration

The Management Console should have a web interface, so the Network Administrator can access the Console from a remote location. This will enable the Administrator to manage the security of a company even while being away from the office.

Rootkit Tracing and Removal

An ideal AntiVirus comes with the power to detect and remove Rootkit components in the system so that Worms and Trojans cannot hide their presence.



Protection against Spyware and Adware

The software must provide continuously updated protection against Spyware and Adware that mushroom in many forms and names every passing day. The software should be capable of repairing damages done to the system by these Riskwares.

Integrated Web Access Policy Enforcement and Management

Policy Implementation and Control

Options should be provided for the formulation and implementation of advanced policies containing many categories for Content Security and Web Access control.

Whitelisting

Once you add a user or IP to the whitelist, content checks will not be done on those entities.

Blocking all inappropriate and non-productive websites

A combination of technologies should be available for blocking all non-productive, harmful and unsuitable websites at a single point. The process of website filtering works on the basis of occurrence of certain 'probable' words like sex, gambling, chatroom and more in webpages. If the word count goes beyond a certain threshold level, then the website in question needs to be blocked and added to blacklist.

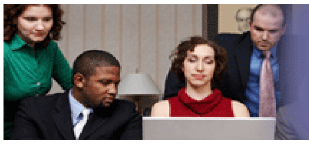
The software must offer default categories like **Pornography, Gambling** and **Ratings Based Blocking.** As an administrator**,** you should have the ability to create as many new categories as required to control the types of websites that you deem unsuitable for the firm.

Pop-Up Ad Blocker

The system must stop pop-up advertisements that plague your computer screen. You must have an option for whitelisting Pop-Ups from specific websites and also have a 'hot key' option to temporarily allow pop-ups.

Protect Privacy and Confidentiality

The application should protect your privacy and prevent access to confidential information. It should be capable of erasing links of visited websites and entries made in online forms. It should allow the user to schedule browser clean-up for Cookies, Plugins, History, Cache, and links to most recent files and images opened.



AntiSpam and AntiPhishing at Mail Server

The security software at the Mail Server should have a Multi-layered Spam Control mechanism. It should include technologies like,

Real-Time Black List (RBL)
RBL is a DNS Server that lists IP Addresses of known Spam sending machines. If the contacting IP is found to be in one of the blacklisted categories, the connection is terminated.

MX / A DNS Record Verification
The domain part of the email address is checked to see if it has a DNS MX (Mail Server) and/or A (IP) record as it is typical of spammers to use non-existent domains in their emails.

Reverse DNS
A reverse DNS check is performed to see if the connecting IP resolves to a valid domain name before accepting or rejecting the email.

Gray Listing
A new email from an unknown sender is kept out for a certain amount of time before accepting it. The logic is that if it is a legitimate mail, the Mail Server will try to resend it, while in most cases spammers won't.

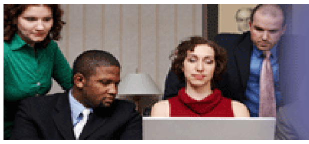
Sender Policy Framework (SPF)
Sender Policy Framework is a world standard that helps to prevent forgery of sender address, and hence works as a powerful mechanism to stop Phishing mails.

Self Learning, Adaptive technology in Spam Control
The need is for a Spam Control system that works on the principles of Artificial Intelligence. It should analyze each mail according to the Behavioral Patterns of the user and take an informed decision based on that. Such a system will show the best accuracy in weeding out Spam.

Now let's check out the requirements of a network firewall.

Protection Against Intrusion and Hacking

The ideal firewall for an SMB network should offer customizable security with user-defined rules for Packet Filtering and Access Control. It must allow the administrator to create Rules based on non-IP protocols such as ARP, whilst supporting multiple network adapter configurations.



Some of the must haves of an ideal firewall for SMBs are given below.

Port Monitoring

It should prevent Port Scanning by network attackers and alerts you of any such attempts. Ideally, the software needs to allow the user to specify Source and Destination ports, and Source and Destination IP addresses. This enables you to enforce Communication Control on specified ports and systems.

Network Data Filtering

An ideal firewall monitors and filters IP and Non-IP Network Traffic so that no intrusion takes place in the company's internal networks.

Active Network Monitoring

You should be able to view details of all TCP connections on your system. Information like Process, Protocol, Local Address, Remote Address, Status and Start Time needs to be displayed in detail.

Filtering Level

It should provide options for Application and Packet Level filtering. Application Level helps you set up Rules for a particular Application. Packet Level provides filtering of incoming and outgoing data packets.

User-defined Rules

The Firewall has to provide a powerful Traffic Filtering system with user-defined processing Rules. Option must allow the users to define Rules according to his or her requirements and implement customized traffic filtering.

Preset Rules

The solution must provide a set of pre-defined Rules so that a newly installed system gets a head-start in enforcing Data Traffic Control. The different types of rules are ARP, DHCP & BOOTP, DNS, E-mail, WWW, News, Net Bios, FTP, ICMP, ICQ, Telnet & SSH, IRC, MSN, and VPN.

Stealth Mode

This option gives you the power to surf the Internet invisibly, without letting other online users see you. When online, your computer constantly receives and responds to information requests from other computers. In stealth mode your computer will not respond to this flow of queries and requests, and thereby reduces the possibility of system hacking significantly.

Comprehensive Logs

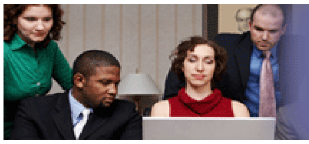
The Firewall needs to store log information detailing programs involved in outgoing/incoming traffic, Communication Protocols used, Source and Destination IP addresses, Direction of Traffic and action taken depending on Rules in force. In addition, it needs to maintain an Event Log that details user events – e.g. changing security levels, loading Rules, firewall shutdown etc.

Real-time Reports

The firewall should provide clear, concise graphical and non-graphical reports on internal and external Data Traffic. Diverse reports based on Application, Expert Rule, Zone Rule, IP and Date are available along with graphs having different styles like Bar, Pie, Line and alike. These reports enable the Network Administrator to quickly analyze the patterns of data movement and to devise strategies based on them.

Conclusion

Threats faced by SMBs are many and multi-dimensional. As aspiring firms trying to make it big in the cut-throat competition out there, it's imperative that mid-sized businesses recognize the importance of safeguarding their Information Systems. A comprehensive solution plan that offers the best-of-breed protection in every aspect of security is the need of the hour. It should provide centralized management, enable Integrated Policy Enforcement and reduce the administrative over-head to a near zero. Once you achieve that, you can safely say that you've got a secure IT infrastructure for your business.



MicroWorld

MicroWorld Technologies (www.mwti.net) is the developer of highly advanced AntiVirus, Content Security and Firewall software solutions **eScan**, **MailScan,** and **eConceal**. **MicroWorld Winsock Layer (MWL)** is the revolutionary technology that powers most of MicroWorld products enabling them to achieve several certifications and awards by some of the most prestigious testing bodies, notable among them being Virus Bulletin, Checkmark, TUCOWS, Red Hat Ready and Novell Ready.

For more information, please visit www.mwti.net