Global Information Assurance Certification Paper

Network Security- A Guide for Small and Mid-sized Businesses

SANS Track 1 Paper
Option 1

Jim Hietala
Submitted October 31, 2004

Abstract

The objective of this paper is to educate both IT staff and senior management for small-medium sized businesses (SMB's) as to the network security threats that exist. The paper presents a digest of industry best practices for network security, which will hopefully assist SMB's in setting priorities for securing the perimeter of a typical SMB network.

The security industry does a good job of publicizing security threats on a continual basis. However, much of what we read in the press contains little if any context associated with each new security threat that can assist senior management or IT staff of the SMB's in determining which threats to address, and in what priority order. This paper will seek to bridge this gap, by providing guidance to companies who, faced with the seemingly impossible and endless task of securing their network, need help deciding where to start, and where to focus- what to do first, second, third, and so on, among the myriad of information security threats that are out there, and possible solutions.

A summary of key actions that are recommended for SMB's is as follows:

- Model the threats to your business, and perform a security risk assessment
- Develop an information security policy, and educate your users
- Design a secure network, implement packet filtering in the router, implement a firewall, and use a DMZ network for servers requiring Internet access.
- Use anti-virus software, both at the gateway, and on each desktop
- Use only Operating Systems that have adequate security baseline capabilities
- Know your network, harden systems by removing unnecessary applications, and maintain an aggressive program of patching operating systems and applications
- Use personal firewalls, particularly on laptops used by mobile users
- Use strong authentication
- Develop a computer incident response plan
- Get started!

I. What are “Small-Medium Businesses”, and why should they care about network security?

Market research firm Penn, Schoen & Berland defines small-medium businesses as being those with less than 1,000 total employees[1].

For many SMB’s, their perception regarding risk of attack is a significant problem in itself. A recent poll by the National Cyber Security Alliance showed that “More than 30% of those polled …think they’ll take a bolt of lightning through the chest before they see their computers violated in an Internet attack[2]”. These businesses evidently believe that they are either too small to be targeted, or too obscure. Or they perhaps believe that they are working in an industry that wouldn’t attract attacks because their data is not high-value intellectual property, or sensitive proprietary data, etc. What these businesses are failing to realize is that in the Internet era, with always on connections providing easy access for mass, indiscriminate attacks, *a business or organization does not have to be a target to be a victim!*

Some very well publicized attacks that were indiscriminate mass attacks include Nimda, Code Red, SQL Slammer, and Blaster, all of which spread rapidly throughout the Internet, and none of which spared SMB’s. In fact, SMB’s may be more susceptible to mass attacks as compared to larger businesses. A case in point is the Mydoom virus (and its many offspring variants), which initially launched in January 2004, and quickly affected one in three small businesses, versus only one in six large enterprises.[3]

Some of the factors that make SMB’s susceptible to mass attacks include the fact that they tend to be pretty homogenous in terms of their computing infrastructure. According to Gartner[4], 90% of SMB’s are running Windows on their servers, 80% are using Outlook and Exchange as their e-mail clients and servers, and 70% are using SQL databases. In addition, SMB’s typically lack the specialized, dedicated, and highly trained security staff that can address IT security. Unlike the situation at large IT organizations, where there is likely to be a significant staff whose sole responsibility is securing the IT environment, at most SMB’s security is likely to be a part time responsibility for someone on the IT staff. Gartner research indicates that more than 60% of midsize businesses in North America do not have a dedicated resource to manage security[5]. The situation at small businesses is undoubtedly even worse.

---

[1] National SMB Market Attitudes Toward Future Growth and the Role of Technology, Penn, Schoen and Berland Associates, Inc., May 11 2004

[2] http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1011092,00.html

[3] Common Sense Guide to Cyber Security for Small Business, Internet Security Alliance, March 2004

[4] http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2914399,00.html

[5] SMBs Show Preference for Security Services, Gartner, 2003

With the proliferation of worms and viruses on the Internet, there is a very high probability that a typical small-medium business will experience an attack. In the same Gartner[6] study, it is predicted that through 2005, 40% of SMB's that manage their own security and use the Internet for more than e-mail will experience a successful Internet attack, and more than half won't know they were attacked.

The regulatory environment is increasingly mandating that businesses of all sorts tighten their security. In industries such as health care and financial services, government regulations (for example Hipaa and GLBA) are forcing affected organizations to enhance their network security and tighten access to personal information. A new law enacted by the State of California, SB1386 (effective July 1, 2003), has implications for SMB's in any industry, and it applies to any business (located anywhere) that sells products or services to California residents. It essentially requires companies that experience a breach in information security to disclose this fact to their customers. A breach is defined by SB 1386 as one in which the confidential personal data of the customer is exposed. Legal experts believe that the bill will open up firms experiencing such a breach to possible class action lawsuits.

Clearly, all businesses need to maintain adequate security, and just as clearly, SMB's are not immune from the security issues that exist in today's interconnected world.

II. Network Security 101- a backgrounder on current security threats, vulnerabilities, and security technologies.

In order to understand the IT and network security environment, and how best to deal with it, it is necessary to define some terms, and describe the kinds of threats and security solutions that exist today. This is not intended to be an exhaustive list, but rather a "plain english" description of the most common terms.

Vulnerabilities- Vulnerabilities are known (or newly found) security holes that exist in software. An example is a buffer overflow, which occurs when the developer of a software product expects a certain amount of data, for example 20 bytes of information, to be sent at a particular point in the operation of a program, but fails to allow for an error condition where the user (or malicious attacker) sends a great deal more data, or unexpected (perhaps special) characters. Vulnerabilities can exist in software running on PC's, servers, communications equipment such as routers, or almost any device running software. Not all vulnerabilities are created equal- some will cause the program affected to crash (which can lead to a denial of service condition on the affected system), or cause a reboot, or in the worst case, they can allow the attacker to gain root or administrative access to the affected system. Upon discovery of a vulnerability, the software vendor will (hopefully quickly) develop a fix, or software patch, and

[6] SMBs Show Preference for Security Services, Gartner, 2003

make it available to users of the software. SANS maintains a list of the Top 20 most critical vulnerabilities that is very useful in ensuring that the highest priority vulnerabilities are addressed.[7]

Exploits- When vulnerabilities are found in software, the hacker community will frequently attempt to develop attack code that takes advantage of the vulnerability. This attack software is called an exploit, and exploit code is frequently shared among hackers, as they attempt to develop different sophisticated attacks.

Threats or attacks- One useful way to categorize security threats or attacks is to look at the intent- a directed attack is one aimed at a single company- for example a company attempting to hack into a competitors network. A mass attack is usually a virus or worm, that is launched onto the Internet, and that replicates itself to as many systems as possible, as quickly as possible. Attacks may come from outside of a company, or a company insider may carry them out.

Viruses- Viruses are generally carried within e-mail messages, although they are anticipated to become a security problem for instant messaging traffic as well. Users unknowingly cause the virus to execute as a program on their system when they click on an attachment that runs the virus program. Virus writers go to great lengths to disguise the fact that the attachment is in fact a virus. They also attempt to spread by using all of the e-mail addresses that they can find on an infected system to send themselves to. An example of a well know virus is the Bagle family of viruses (there have been many versions of this virus). These viruses contain their own e-mail server, so that they can replicate by sending e-mail to all mail addresses that they harvest from the compromised system.

Worms- An example of a worm is the Blaster worm, which rapidly spread through the Internet in August 2003. Blaster targeted computers running Windows operating systems, and used a vulnerability in Remote Procedure Call (RPC) code. Blaster affected computers running Windows 2003 operating system, Windows NT 4.0, Windows NT 4.0 Terminal Services Edition, Windows 2000, and Windows XP. After compromising hundreds of thousands of systems, Blaster launched a distributed denial of service attack on a Microsoft Windows update site.

Trojan horses- As the name implies, these are software programs that are put onto target systems (whether by a direct hack, or as the result of a virus or worm) that have a malicious intent. The Trojan can capture passwords, or provide root access to the system remotely.

Denial of service attacks (DoS)- A denial of service attack attempts to put the target site out of operation, frequently by flooding the site with bogus

[7] http://www.sans.org/top20/

traffic, thus making it unusable. The attacker attempting to create a denial of service condition will oftentimes try to compromise many PC's, and use them to "amplify" the attack volume, and to hide his or her tracks as well. This is called a Distributed Denial of Service Attack (DDoS). Denial of service attacks have now become a popular criminal activity. In an online form of the "protection racket" (pay us some protection money or we'll ruin your business), computer criminals have taken to using denial of service attack methods to put online businesses out of business, at least temporarily, and to then demand money from the target. This sort of cyber extortion attack has been used by hacker rings operating out of Eastern Europe, and has caused significant disruptions to online bookmakers and gambling sites. They are estimated to have cost the industry upwards of £40m ($60-$70m)[8]. Any business that depends on online ordering for a significant portion of its revenues is susceptible to this sort of attack. Denial of Service attacks have also been used to try and put competitors out of business. In a case that surfaced in August, 2004, a satellite TV dealer hired hackers to mount DoS attacks on the websites of his 6 primary competitors, causing them over $2M in lost revenue[9]. Denial of service attacks are very hard to effectively protect against.

Spam- Spam is not a security threat per se, but spam techniques are increasingly being used to deliver malicious software. Spam can also be used to launch "phishing" attacks, which attempt to elicit confidential personal information (bank account information, credit card information, etc.) as a means to steal identity, or cause financial harm.

Some of the more common and popular security industry solutions are described below.

Routers- Routers are perhaps not generally thought of as "security solutions", however most routers today provide packet filtering capabilities, and they can be used to enhance the security of most networks. In addition, there are certain security tasks that are best performed on the router in order to optimize the performance of the overall network, and to reduce the processing load on a firewall.

Firewalls- Firewalls are a fundamental network security solution. Firewalls are used to restrict inbound and outbound network access to only traffic that is allowed by the security policy of the organization. For example, an organization that does not maintain a publicly accessible webserver on their company LAN can use a firewall to define and enforce a security policy that allows outbound web access for employees, but that blocks any inbound webserver access attempts (HTTP protocol, port 80 access) at the firewall.

[8] http://news.zdnet.co.uk/internet/security/0,39020375,39162184,00.htm
[9] http://www.internetweek.com/allStories/showArticle.jhtml?articleID=45200027

Anti-virus software- Anti-virus (AV) software is used to scan e-mail messages looking for defined viruses, which show up as known signatures that the software recognizes as a virus. AV solutions can be implemented on each desktop, or they can be implemented as a gateway or e-mail server function, where all incoming messages are scanned before being delivered to the recipient. Best practices for preventing viruses on a corporate network call for both desktop and gateway or server AV to be implemented, to ensure that laptops that plug into the LAN cannot corrupt systems "behind" the AV Gateway. It is important that both types of AV software are kept up-to-date, as new viruses are found on a very frequent basis.

Virtual Private Networks- The ubiquity and low cost of Internet connections have created a requirement to use the Internet for private company communications, replacing more expensive private networks (frame relay, and private line networks). Virtual Private Network (VPN) technology was developed to allow the Internet to be used in a private manner, with all data between company locations or endpoints being encrypted. VPN's provide privacy for the data while it is in transit across the Internet. VPN's do not secure endpoints from other sorts of attacks, however. And from a security standpoint, VPN's actually extend the corporate network to remote locations. The notion that the network is only as secure as it's weakest link is worth bearing in mind when implementing VPN's, as the weakest link may become the executive's home PC which has a VPN connection to headquarters, or the salesperson's laptop which is equipped with a VPN connection for remote access, or the business partner's LAN that is equipped with a VPN connection to allow sharing of information. Another way to think about this is to acknowledge that the actual network perimeter to be secured extends to all systems that are provided with VPN access- not just those on the local LAN.

Intrusion detection/prevention systems- Intrusion detection (IDS) and intrusion prevention (IPS) systems are products that can analyze certain types of traffic, and determine whether the traffic is legitimate traffic, or if the traffic matches a known pattern indicating that it is attack traffic. An example might be web (port 80) traffic, which a firewall would hypothetically be configured to allow. An IDS system can look at the traffic, and determine that the traffic is actually a NIMDA attack, and not valid user traffic, based upon the pattern. An IDS product will alert on invalid traffic, while an IPS product will block the offending traffic. IDS/IPS products come in two configurations- they are implemented either as a network device analyzing traffic on the local LAN segment, or they are software implemented on a specific host that looks at traffic on that host only.

Spam filtering- Spam filtering can be implemented on the e-mail server, or on a separate appliance sitting between the Internet and the mail server. There are many techniques that can be used to try and identify Spam, and generally the goal is to eliminate as much as possible false positives (legitimate mail mis-classified as Spam), while also eliminating false negatives (Spam that slips past

the Spam filter). A category of Spam that is more ominous than most is what are known as "phishing" attacks. These are generally mass messages that are cleverly crafted to look like legitimate mail from a bank or online merchant, that request the recipient to verify some confidential personal information, usually including account data. Unsuspecting victims who actually respond, and provide their personal information, oftentimes end up the victim of identity theft, or some sort of financial fraud. Implementing a Spam filter will help to improve the security posture of a company, and it will also help to improve the productivity of the company.

The trends regarding threats and attacks have gotten significantly worse over time. Some key trends…

- The time lag from when a vulnerability is found and publicly identified, and an exploit becoming available or an attack being launched has decreased significantly in the past few years. This heightens the need to quickly test and implement software patches that address new vulnerabilities, so as to close the security holes as soon as is possible.
- SANS/Internet Storm Center publishes a statistic regarding the average length of time that a fresh (unpatched) system lasts on the Internet before being scanned or attacked. The latest data available indicates that this time has dropped from 40 minutes to 18 minutes in the last 15 months.[10] This suggests that with all of the various "mature" attacks still floating around the Internet, it is critical to patch new systems immediately upon putting them into service, to avoid being compromised.
- As to the future of attacks, experts have theorized that new attacks will become polymorphic, that is, they will change their code and attack methods over time so as to avoid detection by anti-virus software, and intrusion detection and prevention systems. In addition, a fascinating study looked at techniques that future attacks might use to more quickly propagate throughout the Internet. By pre-scanning for vulnerable systems, and creating a "hit list" of these servers, the study postulates that new worm variants dubbed "flash worms" will be able *"to infect almost all vulnerable servers on the Internet in less than thirty seconds"*.[11] This is significantly faster than previous worms such as Code Red and NIMDA, which required 20+ hours to propagate widely through the Internet. The emergence of this sort of threat will mandate

[10] http://isc.sans.org/survivalhistory.php

11 How to 0wn the Internet in Your Spare Time , Proceedings of the 11th USENIX Security Symposium, Staniford, Paxson, Weaver , http://www.icir.org/vern/papers/cdc-usenix-sec02/

that organizations of all sizes pay very close attention to their perimeter security, and to what traffic their firewall should allow in.

III. Where Do I Start?

It is always dangerous to generalize about what specific set of actions should be taken to enhance security. Each SMB's network and IT situation will be different, with varying levels of sophistication, different types of computers, operating systems, applications, and different access requirements. However, we are making the following assumptions about an average SMB's Internet and IT infrastructure and use:

- They will have an always-on Internet connection, and in addition,
- A mail server hosted onsite,
- A web server hosted onsite,
- A number of Internet users onsite,
- A file server and/or database with proprietary customer and other business information

Given this set of assumptions, there are a number of actions outlined below that will dramatically enhance the security of the SMB's network. Vendor hype to the contrary, there is unfortunately no "silver bullet" in IT and network security. Creating a secure network is only achieved by understanding the nature of the threats that are being faced (and the threat environment is constantly changing), their potential impacts to the business, and by taking those actions that are most likely to address the highest risk threats. It is also important to note security is not a one-off project or exercise. It is probably best thought of as an iterative process- as the threats change, and the IT needs change, new security threats will need to be assessed, and the appropriate security measures put in place.

Top 10 actions to take to create a more secure network

1) Model the threats to your business, and perform a security risk assessment

Because each organization is unique, it is important to think through the potential threats to *your* business. This will be a brainstorming exercise that produces a long list of potential threats. Building upon this list, management and IT staff will then want to think through which of these threats are worth worrying about. A risk assessment will examine all of the relevant security risks, in terms of which risks are applicable to the business, what the expected number of annual occurrences might be for each, and the expected loss per occurrence. This will result in an annual loss expectancy for each identified risk. Armed with this information, it then becomes easier for the

business to decide which risks to address in which order, and what level of remediation expenditure makes sense for each risk. There may be risks where the annual loss expectancy is lower than the cost of remediation, where the business will choose to just accept the risk. The table below shows an example of this sort of analysis.

Risks	Impacts to business	Expected incidents per year	Expected loss per Incident	Annual Loss Expectancy	Remediation steps
Virus infection	Range from time spent cleaning machines to rebuilding machines and loading backup data, and network outage	20	$10,000	$200,000	Gateway and desktop AV
Worm infection	Range from time spent cleaning machines to rebuilding machines and loading backup data, and network outage	5	$10,000	$50,000	Firewalls, patching, personal firewalls for laptops
Hack by competitor	Loss of customer lists, and proprietary information	1	$20,000	$20,000	Firewalls, strong authentication
Theft or disclosure of intellectual property, or confidential data, by insider	Loss of customer lists, and proprietary information	2	$20,000	$40,000	Strong authentication and access control software, audit logs, encryption
Denial of service attack	Loss of use of internet connection, and access to company website	1	$30,000	$30,000	Sophisticated IPS systems, properly configured routers and firewalls, and countermeasures implemented by ISP

The objective of the risk analysis exercise is to identify all of the risks that are relevant to the business, and to rank order them in terms of priority. The risks and their priority will be different for each business. A small company that does all of its business via Internet ordering will necessarily want to make certain that the web server hosting the order processing application is secure, as 100% of the revenues of the business rely on this server and software. Similarly, they will place a high loss expectancy value on denial of service attacks, as these can cause a significant loss if the ability of customers to place orders is affected. A “brick and mortar” company that uses the Internet for less critical functions is certain to have different risks and priorities. A company that maintains multiple branch offices, all with VPN connections to the corporate headquarters, will have different risks than a company which does not have remote offices, and which does not extend VPN access outside of the main office. This is why it is critical to evaluate the specific risks to your business.

It is also advisable for SMB’s to stay abreast of emerging threats and vulnerabilities. There are many industry newsletters and security industry websites that can be of assistance, including:

Http://www.sans.org

Http://www.securityfocus.com
Http://www.securitypipeline.com
Http://www.esecurityplanet.com

SANS publishes an annual list of the 20 most critical vulnerabilities[12]. This list presents a consensus of industry experts as to the most critical vulnerabilities for Windows and UNIX systems. This list is worth reviewing (it is currently updated annually), to ensure that any vulnerabilities present in the SMB's IT infrastructure are addressed via patching, or some other solution. The list provides detail on the nature of the vulnerability, it provides guidance on how to determine if you are vulnerable, and most importantly it tells you how best to address each vulnerability.

2) Develop an information security policy, and educate your users

Every organization of any size should have an acceptable use policy for their computing resources, defining how employees may use IT resources, including the internet, and an e-mail policy, defining acceptable uses and practices for company e-mail. SANS has a great resource, the SANS Security Policy Resource page[13], that can speed the development of sound information security policies. The web page contains templates for many areas where an organization may need to develop a security policy. Templates for these and many other security-related IT policies can be found on the SANS website.

Creating a set of clear security policies and making the organization aware of the policies will provide a foundation for a secure network. For example, defining a policy that requires all software to be used on company computers be first tested and then implemented by IT staff, and making end users aware of this policy, will reduce help desk calls, and will strengthen security. Similarly, defining and enforcing a corporate password policy will strengthen security. It is also important to undertake user education on company security policy, so that users understand their part in maintaining the security of the company's network and IT resources. Users need to fully understand their role in the security process, which extends from "don't open attachments from people you don't know", to not sharing passwords, and using strong passwords. The risk assessment recommended above will likely highlight areas where security policies need to be developed. For example, when a company extends network access via a VPN to third parties (business partners, suppliers, consultants, and so on), it is advisable to have policies for what sort of network traffic will be permitted from the remote site, and what sort of security solutions will be in use at the remote site, including firewalls, anti-virus, and so on.

[12] Http://www.sans.org , The 20 Most Critical Internet Security Vulnerabilities
[13] Http://www.sans.org/resources/policies/

3) Design a secure network, implement packet filtering in the router, implement a firewall, and use a DMZ network for servers requiring Internet access.

There are many considerations in designing a secure network. Some of the key factors to consider include the following:

- Use a "defense-in-depth" strategy in designing a secure network. This basically means not relying on a single device or product to enforce security, but instead using the security capabilities of a router, and firewall, and ensuring that software on hosts and servers are up-to-date with patches. In more sophisticated environments, it may also mean that some or all of the following advanced security solutions might be called for- intrusion detection/prevention devices, host intrusion prevention software, application firewalls, or encryption solutions.
- Implement a firewall- ideally one that provides stateful packet inspection. Given the set of assumptions provided earlier, the firewall will need at least three interfaces- LAN, WAN, and DMZ. The LAN interface will be used to connect all of the user workstations, and Network Address Translation should be used to hide the actual addresses of all workstations. The mail server and web server will be placed on a network segment using the DMZ interface, where the traffic into and out of these devices can be subjected to different filtering rules. Address translation should be applied to these devices as well.
- Consider implementing application proxies for common applications and protocols. Proxies provide additional security by not exposing internal hosts to the Internet. This includes web protocols, and e-mail.
- Use the "principle of least privilege" in determining appropriate access to network resources. This essentially means that if a given group of users, be they internal or external, do not need access to certain systems, or applications, then they should be restricted from this access. A simple example is a payroll system. In most companies, very few people in the company will actually need access to the payroll system. Given a properly designed network, it is possible to use a router or firewall to restrict access into the payroll system so that it can only occur from the IP addresses of workstations with a legitimate need for access, and access from every other workstation is restricted and blocked.
- Test each of the components after installation, to ensure that they are performing as expected. For example, test to ensure that a firewall that is configured to only allow inbound web access to the web server located on the DMZ actually blocks other attempted web access, to other hosts. A study of firewall configuration errors concluded that almost 80% of firewalls examined had "gross mistakes" in their actual implementation.[14] Thus the necessity of testing the firewall and perimeter security. Ideally

[14] A Quantitative Study of Firewall Configuration Errors, Avishai Wool, IEEE Computer Society, June 2004, http://www.eng.tau.ac.il/~yash/computer2004.pdf

the testing will be done by someone other than the person or organization that configured the firewall and perimeter security. Testing and validation of the configuration is done using various scanning tools (many of which are freeware), and is important to ensure that no inadvertent “holes” have been created in the security of the network. Beyond configuring the correct policies and rules in the firewall and access router, it is also very important to setup the devices in a secure manner. There are many commands and setting in each of these devices that can introduce security exposures and weaknesses if configured incorrectly. An example would be turning remote Telnet access on in the access router. All routers support this, but security “best practices” would say to disable this capability, and if it is necessary to be able to access the router console via the Internet, at a minimum use a more secure option such as SSH.

A great resource for IT personnel tasked with designing and implementing a secure network is the SANS reading room, accessible at Http://www.sans.org. This public resource has many secure network designs submitted by certification students. All certification papers are public references, and a great deal can be learned from referencing these papers. Papers have been written for almost every brand of firewall, and for many different network configurations.

4) Use anti-virus software, both at the gateway, and on each desktop

Given the proliferation of viruses, using AV software is a must. Implementing gateway anti-virus software will ensure that all incoming and outgoing e-mail is scanned for viruses. It is also wise to consider blocking some categories of attachments (i.e. those that can introduce a virus or Trojan, for example .exe files and other programs, scripts, and even .xls and .doc files that can contain harmful macros).

Using AV software on each desktop is also recommended, as any viruses that get introduced from somewhere other than the Internet can be caught at the desktop (for example a laptop user picking up the virus while at home, and then spreading it upon reconnection to the corporate network).

5) Use only Operating Systems that have adequate security baseline capabilities

For example, Windows 98 and prior versions do not have a real login capability- user Ids and passwords that are used can be easily bypassed just by hitting “esc” at the login prompt. This is fundamentally unsecure. Upgrading to Windows 2000 and beyond provides real login/access control capabilities, which are essential. In addition, as Microsoft is no longer providing patches for Windows 98 and prior releases, any security vulnerabilities that are found in these older OS’es won’t be fixed/patched.

It is also recommended that users not be given administrative privileges on their systems, and that the systems be delivered to end users in a "locked down" configuration, where users are not allowed to load on any additional software.

6) Know your network, harden systems by removing unnecessary applications, and maintain an aggressive program of patching operating systems and applications.

It is important to know what is running on each system on your network, and to ensure that appropriate patches are applied. The SQL Slammer attack took advantage of a vulnerability that was known for more than 6 months, and for which a patch was available for more than 6 months. Frequent patching will reduce the exposure from newly found vulnerabilities. This is very important, as the time lag between vulnerabilities being found and exploits and attacks being launched has shrunk significantly in the past few years. Many organizations that were affected by SQL Slammer thought that they were immune, as they weren't aware of having SQL database installed. In some cases, these organizations had a proprietary application that used an SQL database, and as a consequence they were affected. Knowing your network, hosts, and operating systems is a matter of knowing what is running on each system, the vulnerabilities that exist in the OS version, and of maintaining a secure configuration. There are many tools that can be used to assist in this effort, including:

- Microsoft Baseline Security Analyzer[15]
- Nessus[16]
- NMAP[17]

All company servers (mail servers, web servers, file servers, databases, etc.) should be hardened by removing unnecessary software and processes from the systems. For example, default installation of several operating systems will turn on all sorts of programs and services. If the program or services isn't needed by the business, the prudent thing to do is to remove it. This will tighten the security posture of the company by providing fewer avenues for attackers to try and exploit.

7) Use personal firewalls, particularly on laptops used by mobile users

Laptop PC's that are sometimes used in the office and at other times used while connected to foreign networks have proven to present security

[15] http://www.**microsoft**.com/technet/**security**/tools/mbsahome.mspx
[16] http://www.nessus.org/
[17] http://www.insecure.org/nmap/

problems. These laptops may be used on dial-up networks, wireless LAN's, or home broadband networks. When the Blaster worm attack was launched, many businesses that had implemented firewalls on their Internet connection believed they were secure, and they were- in terms of access via their Internet connection. Many of these same businesses were infected by the worm when a laptop user picked up the worm while connected to a foreign network, and then subsequently connected to the corporate LAN. Upon connection to the company LAN (behind the firewall), the worm quickly sprayed itself to the entire company. Personal firewalls implemented on (at a minimum) company laptops will address this security hole. For laptops that contain highly sensitive data, using strong authentication and even encryption will reduce the possibility that company data is exposed, even if the laptop is lost or stolen.

Several third party firewall products exist to address this need. For users of Microsoft's XP OS, the new Service Pack 2 release includes a built-in firewall module.

8) Use strong authentication

Left to their own devices, most users will pick short and frequently predictable passwords. There are many attack tools that try to guess user ID/password combinations, based upon a brute force approach (trying every possible combination) or that use a dictionary approach (trying common words from an electronic dictionary). Many operating systems provide the ability to force minimum password standards, including length (longer is better), avoidance of using dictionary terms, and use of special characters (using punctuation characters, for instance, makes passwords less susceptible to dictionary attacks). Anything that can be done to avoid using standard dictionary words will help to improve security with regards to authenticating users. In addition, many solutions exist that can enhance authentication through the use of security tokens. These products use cryptographic techniques to produce "one time" passwords. This is referred to as "two factor" authentication, wherein users are only permitted access after verifying "something you know" (the valid user login and PIN), and "something you have or possess" (the security token that produces the one-time password). A third approach for the truly paranoid can include "something you are", or a unique biometric characteristic such as a fingerprint.

9) Develop a computer incident response plan

Even small companies need to think through how to respond in the event of a security incident. The computer incident response plan should identify the resources that will be involved in analyzing the incident, and the plan for analyzing and recovering from the incident. For small businesses, the

resources that are called in may be external resources, for examples consultants or integrators. Here is a real world example- one evening your ISP calls and tells you that an IP address that is registered to your company is sending out massive amounts of SPAM, and that they will be removing your internet access until the problem is solved. If your business depends on the Internet in any way, you will need a plan to analyze what is happening, identify the resources that have been compromised, pull them offline, clean and rebuild the systems, and resolve the problem ASAP.

10) Get started!

Businesses of all sizes frequently only get serious about security after experiencing an attack or incident of some sort. While a harmful virus or worm can be highly motivating in terms of making an SMB focus on information and network security, it is inarguably better to expend resources and energy before an attack happens, and to periodically review and strengthen the security measures in place.

IV. Conclusions and final thoughts

The downside of trying to condense the topic of securing a network to a "top 10 actions" list is that the result will inevitably leave out some very important actions. Businesses should, in addition to the 10 actions listed above, also have a business continuity plan that looks at business-impacting disasters and plans for and tests responses. SMB's should backup critical data frequently, and test that the backup/restore process actually works. SMB's should also evaluate their physical security- looking at how access to physical IT equipment is controlled and secured. They may also want to consider having an outside organization actually test their security- this is called a penetration test, and can help to identify security problems and weaknesses.

Security is worth investing in. The downside of doing nothing may well be that the business ceases to exist when a malicious attack destroys customer records or valuable proprietary data. However, addressing the problem needn't necessarily mean hiring direct, expensive staff. There are many great security systems integrators and managed security service providers who can assist an SMB to implement the appropriate solutions. When considering using a third party to assist with solving security problems, it is important to make sure that the organization has qualified personnel, and proven expertise. One way to ensure that this is the case is to look for partners who have recognized expertise in information security- with respected certifications such as the SANS/GIAC certification series (GSEC, GCFW, GCIH, et al), and the ISC2 CISSP certification.

List of References

The following materials were utilized in researching this paper.

SANS Institute, Track 1 SANS Security Essentials And The CISSP 10 Domains, Version 2.2, January 2004.

Bruce Schneier, Secrets and Lies, Wiley Computer Publishing, 2000.

Penn, Schoen and Berland Associates, Inc., National SMB Market Attitudes Toward Future Growth and the Role of Technology, May 11 2004.

http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1011092,00.html

Internet Security Alliance, Common Sense Guide to Cyber Security for Small Business, March 2004.

http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2914399,00.html

Gartner, SMBs Show Preference for Security Services, , 2003

http://www.sans.org/top20/

http://news.zdnet.co.uk/internet/security/0,39020375,39162184,00.htm

http://www.internetweek.com/allStories/showArticle.jhtml?articleID=45200027

http://isc.sans.org/survivalhistory.php

Staniford, Paxson, Weaver, How to 0wn the Internet in Your Spare Time , Proceedings of the 11th USENIX Security Symposium, http://www.icir.org/vern/papers/cdc-usenix-sec02/

Http://www.sans.org/resources/policies/

Avishai Wool, A Quantitative Study of Firewall Configuration Errors, , IEEE Computer Society, June 2004, http://www.eng.tau.ac.il/~yash/computer2004.pdf

http://www.**microsoft**.com/technet/**security**/tools/mbsahome.mspx

http://www.nessus.org/

http://www.insecure.org/nmap/

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event