Global Information Assurance Certification Paper

Maximum Security in Small Business

Cody Ray
Security Essentials Certification Version 1.2c

Information security is making the headlines. The Internet community and the press are focusing more and more on hacker attacks and virus outbreaks. In response to this phenomenon, big business is making a move to provide security appliances and more robust security offerings. The response has been a positive move for the security professional, but small businesses seem to be suffering. Small businesses can't seem to justify the amount of money that is needed to build a secure infrastructure for their business. In a time when small businesses are booming and there are more small business dollars being made than big business in corporate America, security seems to be falling through the cracks. At the same time small businesses are finding freedom on the Internet and increasing their market presence through online advertisement and websites. These storefronts need to be protected. One must protect that website, stay current on exploits, monitor traffic to and from their network and stay current with technologies. That is a lot to ask a small business owner. Considering the typical size of a small business staff ranges from 25 to 100 users and there is, on average, one system administrator (if you are lucky), there is a lot of work to be done to centralize management help. So what is a small company suppose to do? Can they afford a security program? Can they protect their business in an efficient way?

The answer is a complicated one indeed. Lets answer that question with two very important questions, "How important is my data to my business?" If lost or compromised, can I survive as a business? If you answered either of these questions with a "no" then security is a must.

Most businesses now have a dedicated connection to the Internet in the way of DSL or a cable modem. These "always on" connections are fast and perfect for the small business, but because they are always on they usually require a static IP address. This fact makes them easier targets for attackers and provides an identity footprint of the business. Firewalls are the first step to protecting this static gateway. The SOHO (small office / home office) market for firewalls is flourishing. Vendors such as SonicWall, Watchguard and free software host based firewalls such as Zone Alarm are targeting products to these markets. SonicWall provides a firewall that incorporates multiple services such as packet filtering, NAT (network address translation), virus scanning, VPN (virtual private networking), reporting and remote management. This solution is cost effective for a small business and provides adequate security by blocking unwanted packets from coming into the LAN. The fact that NAT is used is also a plus. NAT hides the internal network from the Internet by using reserved private addresses that are not intended to move across the Internet. It then assigns one or more public IP address on the external network to use as a means of translated transport. This provides a layer of protection by not allowing direct access from the Internet to the internal network.

I have evaluated and tested both the Watchguard firewalls and the SonicWall firewalls. There is a definitive difference between the two products that I would like to go over. The major difference between the two products is the price. Watchguard makes a

less expensive firewall solution in the SOHO arena than SonicWall. There are hidden costs however that the consumer should be aware of. Watchguard gives you free upgrades to its firmware for a year, but then a cost ensues after the yearly period. SonicWall provides free upgrades for the life of the product via it website. In fact, you don't even have to log into the website to receive them. Both firewalls support content filtering, but during tests the SonicWall SOHO unit outperformed the Watchguard SOHO unit by a large margin. One of the reasons for this is the fact that the SonicWall handles more simultaneous connections than the Watchguard product. When using NAT, a connection behind the firewall is taken and masqueraded as the public IP address of the SOHO unit. The connection is then allowed to pass over the Internet. It stands to reason that this can only happen so many times until physical memory of the unit is saturated while trying to keep up and thread these connections. When too many connections are attempted, the performance of the firewall appliance suffers. In the case of the Watchguard SOHO this happened immediately after content filtering was enabled. The reason for this is simple. A browser makes approximately twelve connections per instance and per user when launched to read a website. When content filtering is enabled more connections are made to help assist the firewall in knowing if the site should be blocked or not. The actual numbers, obtained by the two companies are as follows: SonicWall SOHO2 maximum connections equal 3072 without content filtering and 1544 with content filtering. Watchguard support claims that their SOHO will handle 999 connections without content filtering. It should be obvious after comparing the numbers stated that the SonicWall SOHO2 outperforms the Watchguard SOHO when content filtering is enabled.

VPN technology is another way to increase business efficiency and provide security. VPN (Virtual Private Networking) provides mobile employees with a secure connection over the Internet to the business. This provides a way for employees to work securely from anywhere in the world as long as they have a connection of some sort to the Internet. This is ideal for replacing those RAS (Remote Access Servers) boxes out there. Not only can you provide a more secure connection by not allowing unencrypted dial-ins, but it is cost effective as well. Info World reports, "Because VPNs were once prohibitively expensive and relied on dedicated lines, they used to be limited to the largest of corporations. But the advent of low-cost hardware, coupled with less-expensive broadband connections, has made many CTOs rethink how best to handle secure remote connections; VPNs now look especially good for connecting the remote employee's SOHO (small office/home office)." In fact, it is the best way to control and implement connections to your network. When a VPN connection is made with a software client the connection is manipulated in such a way as to put the remote computer on the internal LAN with an internal IP address. The network appears as if you were actually on campus!

As much as VPN is attractive it also brings forth some unwelcome side effects. Keep in mind that you are bringing remote users into your network and placing on the internal network as if they were in the office. This means you must treat them as if they were on campus. They must follow the same security practices and you must make sure there are no vulnerabilities on their remote machines. One example is to ensure proper virus scanning software is installed and kept up-to-date. This brings us to another

sometimes-overlooked necessity of the small business security arsenal, virus scanning.

Viruses are plentiful and extremely damaging to work efficiency and data. The Melissa virus and Love Bug virus are just two of the millions of viruses out there. They are mentioned because they are two of the most well known. These two viruses were able to replicate rapidly and cause millions of dollars of damage to businesses worldwide. Virus authors have brought entire companies, small and large, to their knees in recent months by compromising the very core of communication, email. These malcontent hackers target e-mail systems as a way to replicate their work easily. Viruses should be easily combatable in a small business environment and with the headlines bulging with the news of such attacks, awareness should be relatively easy to acquire. The network administrator should inform users of new viruses and educate them to not open strange attachments or attachments with executable extensions (.exe). They should disable macro use, unless required by job function and keep virus software up-to-date. Virus scanning software can be managed from a central server or firewall (SonicWall uses the McAfee engine). With prices for small business security packages ranging from three hundred dollars to five thousand, depending on what you want to do, it would appear to this author that these fees pale in comparison to the amount of loss one e-mail worm could cause. In fact, in his book entitled *Tangled Web*, author Richard Power documents that the creator of the Melissa virus, David L. Smith, admitted in court to causing $80 million in damages.

> "Why $80 million? Well, it's simply the upper end of the scale for damages used in the federal sentencing guidelines. The actual losses related to Melissa were reported to be hundreds of millions of dollars, but once the toll reached $80 million, those prosecuting the case had all they could want or even use in order to impress the court. The Melissa case had reached the outer limits of what was even conceived of in the federal sentencing guidelines."

Mr. Smith's statement here proves the cost effectiveness of a well thought out virus protection program and policy. It also proves that defenses should always be upgraded and policies should always be followed. It was to be only one year later that the Love Letter worm replicated through the same paths as the Melissa virus.

To some network administrators, the first line of defense may be thought of as the firewall, but I believe it to be the almighty password. Passwords are important for keeping unauthorized people out of your systems but their importance is beginning to fade. Weakened password policies will most assuredly cause any security policy to lose its effectiveness, thus creating a weak foundation to any company's defense. In today's computer world where processors are in the gig hertz range and the utilities are plentiful, cracking passwords has become nothing more than a slight nuisance to the common hacker. In a smaller business enforcing a strong password policy should be easier than in a larger corporation. However, one must combat the "everyone is a friend" environment in which employees share and give out their passwords to co-workers. One-way to explain this is to tie activity and responsibility to the username. If a username was logged doing something inappropriate the employee responsible for the username should be questioned and held somewhat responsible. Keep in mind that a hacker could have stolen

the password and username and masqueraded as the individual. For this reason passwords should be alphanumeric and use special characters to complete at least a six-character length password. Password auditing should be done at least once every three months and I would recommend once every month. A common tool used to audit Windows NT is L0pht Crack. According to L0pht, "...password auditing is the only sure way to identify user accounts with weak passwords." The administrator should always get permission when doing password auditing and should practice adequate backup procedures before modifying or playing with the password files of the operating system.

Please note that tying a username to unwelcome activity on your system may not always lead you to the culprit. Logins can be stolen by cracking the password of the user and then the login account can be used to masquerade the true identity of the intruder. One way to overcome this situation is to use Smart Cards. I will not cover Smart Card usage or implementation in detail because I do not feel it presents itself as a cost effective small business solution. The small business managers I have spoken to approve of the idea, but cannot justify its implementation in the work place and would rather deal with password enforcement through policy.

This leads us to the biggest, yet in some cases most difficult measure in small business security, policy, policy and more policy. As with any business, employer protection from lawsuits and employee protection are a major focus. Developing policy is a must for this type of protection. The Human Resource Department of your organization is probably all too familiar with the downfalls and successes of business policy. Developing a security policy for your organization can serve as added security when faced with an internal violation or incident. However, if the policy is not created correctly it may serve as more of a hindrance than a solution. Remember that policy should be written to be flexible and changeable. The policy should be broad enough to encompass what needs to be covered in your organization and it should be to the point. A short policy that lays down the law is much more effective than a policy that takes employees twenty minutes to read and a lawyer to decode. Keep it simple.

When writing a security policy, take time out to look around your business and watch what the employees are doing. Note the security flaws and what can be done to improve them. For example, if employees are spending a lot of time sending personal e-mails, write a policy that limits this or discourages this practice. Remember, e-mail is one of the primary transports for viruses and is usually hidden in a more socially based message and is usually sent between friends. Another classic example is non-work related web surfing. If you notice that employee efficiency is suffering because people are surfing the web to non-related sites you may want to consider writing a policy addressing what are acceptable sites and what sites are considered inappropriate. One such way of enforcing this type of policy is to use content filtering on your network through a firewall gateway (Sonic Wall SOHO units have this ability) or through a proxy server.

There are a number of references on the Internet regarding security policies and there are even some prewritten examples. PentaSafe (http://www.pentasafe.com) is a company, which has developed a product, *VigilEnt Policy Center,* which solely focuses on the development of security policy. They have really focused on trying to make the entire processes easier yet robust at the same time. If you are having problems coming up

with a good policy or feel intimidated by the process, PentaSafe's product is definitely the answer. There are a number of examples on their website regarding why policy is a must in today's Internet world. I have one excerpt from their site, which signifies my points mentioned above;

> An oil company computer technician compiled a list of jokes about sex. Proud of his list, he broadcast this list on the Internet, appending his electronic mail address to the end, just in case the recipients happened to have heard any new ones. Management was able to have the posting deleted from several discussion groups, but was not able to control copies that had been made. Around the same time the same technician had printed a copy of his list, and when distracted by something else, had left it in the hopper of a departmental printer. Women in the department objected that they had been subjected to sex jokes via email that they didn't want to hear. They pointed to the Internet postings and the printer output as examples. The pending sexual harassment lawsuit was settled for an undisclosed sum. A policy about permissible use of the Internet, as well as a policy about representations made using the company name on the Internet were noticeably lacking.

It should be clear that a well-written policy could provide a small business enterprise business protection at a very small price.

Ah, the ever looming price. Security is not cheap in this day and age, but the cost can be controlled with proper implementation. Security can also be proven cost effective. With the adjunct of the Internet and "always on" connections this has never been truer. According to CERT/CC statistics, the year of 1999 produced 9,859 reported incidents, the year 2000 produced 21,756, and the year 2001 has already produced 7,047 incident reports in the first quarter alone. Computer security incidents are growing exponentially every year making security spending as much a part of a businesses allocable expense as the electric bill. Most think it will never happen to them. Most say they have nothing to hide. Wait until it happens. The feeling that your business is vulnerable and out of your control is not a feeling wished by most. Taking a chance in an increasingly vulnerable world lessens your odds for survival. In a free market economy were knowledge, performance and integrity say something; wouldn't it be nice for it to be you saying it rather than a teenager expressing it through your now tainted website? Take initiative and make security a concern. Follow the information in this paper and develop a small business solution that works for you and your business. Make information security the foundation of your infrastructure and watch your business grow. This foundation, if correctly formulated, will keep those teenagers self-expression talents in freshman art class and out of your livelihood.

References

Fielden, Tim Info World – "SOHO VPNs bring secure connections to all." May3, 2001 WWW: http://www.infoworld.com/articles/tc/xml/01/05/07/010507tcsoho.xml (May 5, 2001)

Power, Richard. *Tangled Web*. Indianapolis. IN: Que, 2000 p.145

L0pht. ::LC3::. WWW: http://www.securitysoftwaretech.com/lc3/ (May 16, 2001)

PentaSafe. WWW: http://www.pentasafe.com (May 4, 2001)

CERT/CC Statistics 1988-2001. WWW: http://www.cert.org/stats (May 15, 2001)

Last Updated: July 25th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event