Global Information Assurance Certification Paper

Security problems for small companies

Jeremy M. Klomp

Practical version 1.2f

November 6, 2001

Overview

A growing problem in our technologically advanced society is the increase in security related issues for small to medium sized companies. Government regulations now require financial, health care and many other types of industries to meet stringent security requirements and many of the smaller companies are struggling to meet them. With the increase in security related incidents over the past few years, companies are struggling to maintain a secure network infrastructure. Internally they often lack the staff and resources to secure their IT assets and therefore struggle to preserve a secure network. This is causing small businesses to become a security hole themselves because many hackers attack them because of the low security that most companies have and then launch bigger attacks on larger organizations. Just this year alone, CERT's (Computer Emergency Response Team) incident tally should top 46,000 for the year, more than double the 22,000 incidents reported last year causing even greater concern (Luzadder, 2001).

Many businesses are often oblivious to these security issues until the business itself is affected. Most often they lack well-trained staff, which results in gaping holes in the security structure and leaves the company at great risk of being compromised. After a business is compromised, they are often used to launch attacks on bigger companies leaving the small businesses open to lawsuits, data loss, having to spend large sums of money to fix assets after being penetrated, and more importantly it leaves their business open to attacks that could put the company at risk of being shut down.

Although many businesses do not realize it, the security problems begin the moment the business has a presence on the Internet. This presence might be something as simple as email for the company sales staff or something as complex as web servers used to sell their products. Small businesses who use the Internet have grown 46% faster than those that do not (Internet Indicators, 2001), making many companies jump on the Internet bandwagon without thinking about the consequences. This simple Internet presence often causes companies to leave themselves open to numerous security problems. Many of these issues are "invisible" to inadequately trained staff and often these companies do not have the policies in place to deal with security problems and IT issues you will have by doing business over the Internet.

There are many steps a company can take on a daily basis to keep their assets secure. With the advent of new viruses such as Nimda and code red**,** September 11th terrorist attacks, hacker attempts, and many security holes in the applications being used on the Internet, small businesses job of securing their resources is even tougher. Many companies are just struggling to stay in business and do not have the resources to apply to security for their computer systems. There are many things they need to do to make sure they are secure and are being proactive about maintaining this security. Some of those include virus software, backups, security updates and

patches, firewalls, reviewing network designs, having best practices for ongoing issues, having policies in place to deal with problems, having some form of change management to make sure security is being thought about, and the many regulations that companies are beginning to face in the industry and by government.

Security problems for small businesses

With recent attacks on high-profile Web sites in the news, computer security is a growing concern for many small-business owners (Feuer, 2000). Many of the problems for small companies stem from the lack of knowledge when setting up new equipment. Many times companies will have consultants or staff members install new equipment and most often security is not a primary concern of the project leaving a large problem to be dealt with later. This often leads to several problems later on with hackers, viruses, data recovery and many other security issues. The biggest challenge is finding people with the knowledge and understanding of security so that the projects are done right the first time and then having the policies in place to maintain security.

The largest and most destructive of security problems is viruses. Viruses are becoming the number one issue for most small companies and are one of the most destructive as well. Viruses have been around for a very long time, but until recently they were not taken as seriously. As virus writers became more creative and many viruses exploited multiple security holes they became more and more destructive affecting many companies physically as well as financially. Recently, there were major virus problems exploiting secure holes in Microsoft's IIS (internet information server) and infecting other machines on the computer network. These viruses infected many critical files on file servers and web servers. This generated a large amount of traffic on the Internet slowing down many company's networks. With the Nimda virus, virus protection just was not enough because it exploited ISS security holes, which if left unpatched, would infect those systems and then spread throughout the network thru drive mappings. Just one system with the vulnerability open caused the network to be affected. Mcafee, for example, released updated DAT (data) files, but they deleted files instead of cleaning them causing massive data lose for a lot of companies. Many small businesses were caught off guard from the latest round of viruses and are considered extremely vulnerable because they aren't staying on top of virus DAT updates and security updates on their software. Another example of this is the Code Red virus. Many small businesses use DSL (digital subscriber line) connections and leave their DSL routers with the default setup causing port 80 to be listening and causing them to be very vulnerable to a virus that targets port 80 like the Code Red virus. Many companies could not keep their Internet connections up and running because of this virus and lost the vital Internet connections they require to do business. Qwest themselves had a major problem with this and did not come out with a fix for days after.

The next large security issue is introduced when a business uses a web server either for ecommerce or for something such as hosting the company web page. Often they are installed for small businesses by consultants or staff who just install the servers and get everything working. Many times security is put on the back burner in this situation. Everything looks good from a functionality point of view, but many times are left wide open from a security prospective. Security updates come out all the time for IIS, which is one of the most commonly used web

server software on the market, and many companies do not even know about the patches and secondly do not know how to apply them. This leaves their company open to attack. Hackers and virus writers are on top of the most recent patches and know that a lot of companies do not patch their servers right away and they take advantage of that and use those holes to launch attacks on those companies not patched. Many then use those compromised systems to attack bigger companies, or even the whole Internet as we have seen recently.

There are many companies that do not have any firewalls and they pay the price many times by getting their web pages defaced or get their servers used to launch attacks on other companies. But as firewalls are becoming commonplace with most small businesses they are still the devices that are a big mystery for most companies. It is the box that sits in the rack and runs, which gives them a false sense of security because they feel it is all they need to do to keep protected from security intrusions. There are many companies who have their firewalls configured incorrectly by leaving large numbers of ports open to servers or are allowing servers which do not need to be accessed from the internet to be open to it. If configured correctly these devices are very effective against attacks, but if done wrong they can leave vital devices open to attack without knowing it.

Instead of fixing buggy software, the focus should be on locking down computer systems to prevent activity that could be compromising (Becker, 2001). Incorrect network designs a lot of times can lead to problems as well. If a new server is brought online or a new office is opened up, then there needs to be a review to address the security that is needed. To many times a company will open up access to a server in another location to the internet thru the corporate location and leave the hole open in the firewall into the internal network of the company not realizing that the server is not patched. This leads to major problems. If a web server is needed it should be put in the DMZ (demilitarized zone) at the corporate office to restrict access to internal networks to minimize any damage intrusions on those servers may have to internal devices.

A tape backup system is a lot like an insurance policy (Feinberg, 2001). Backups are considered by many to be the most essential security precaution a company can do. Backups are a difficult thing to keep on top of because of the many issues backups have. A lot of companies feel that they are getting their data backed up without a problem only to find out they have their backup software configured wrong and end up with no data to restore when it is needed. Backups need to be check on regularly and logs need to be looked at daily for any errors that have occurred. Some companies may have regular backups occurring, but a lot of them may not realize that you need agents to backup open files and databases to ensure that all data gets backed up. Small companies just do not have the expertise to deal with these problems and many times don't realize it until it is too late.

Systems managers should develop a list of best practices that are specific to their application mix and the components of each of the applications (Bassett, 2000). There are many best practices that companies need to do to keep major problems from happening to their networks. Virus updates and settings, backup tapes changing and checking of backup errors, security updates tested and installed, firewall configurations evaluated, defragging of databases (exchange, arcserve, etc), scanning of networks for holes, checking guidelines for setting up servers and

network devices, and event log checking and researching are just some examples. Finally, and perhaps most important of all, is the need for you as an administrator to constantly study and follow the latest security warnings and alerts as they are published (Hall, 1996).

Having the policies in place to deal with security related issues are probably the simplest things a company can to do insure that companies are keeping their infrastructure secure. Most companies have policies for employees to follow, but a lot of the policies are passed on by word of mouth in a small business. These policies need to be written down and signed off on by all new and existing employees so they know what is expected from them and so the company can limit its liability. Having good policies in place can protect the company against it's own employees and hold them accountable for what they do. It is stated by numerous places that the biggest security threat to a company is it's own employees. These policies are in place to keep devices secure after they are secure initially and so any changes to network infrastructure should go thru a change management process to make sure the security aspects are addressed and to make sure people are constantly thinking about security when making changes. One change done without security in mind can create a large hole in the security of the company and put it's own data at risk. A large part of policy making is creating guidelines on what to do in the event of an intrusion or disaster. In the wake of September 11th and what has happened to so many companies in the world trade center, people are finally taking disaster recovery and data recovery very seriously and make that an intrical part of their security plans. You can put all the policies in place, but one major event can destroy a company if the policies and plans are not thought thru and maintained.

There are many regulations that companies small and large must now follow as well. Many financial companies, banking companies, hospitals, and government agency must all follow strict guidelines and perform audits yearly to make sure the computer security is as good as possible (Sungard). Many of these companies can face fines and other repercussions because of not meeting those guidelines. There are also many new guidelines being discussed by Congress and other regulating bodies in the wake of September 11th to make security and computer security a lot higher so that in the event of an attack, companies are well protected and sheltered from any damage that could be done to the companies themselves as well as financial markets in the event of a large attack on the United States computer systems. All of this takes time and resources for companies to get their systems up to grade and to keep them secure as an ongoing practice. Data is the most important piece to a company's well being and keeps many of the trade secrets and should be treated as such.

Outsourcing to Managed Security Service Providers is key

One the best things for small business's is outsourcing the security of their computer networks. The fact is, unless your network is constantly monitored, patched, and improved, security problems will go unnoticed and lead to major problems. One of the best ways of dealing with this ongoing need is to outsource it to companies that specialize in security such as a managed security service provider. They are able to handle new tasks with speed and reliability while maintaining the critical applications and data you have already got. Simply put, securing networks is there business. They give a small company the optimum combination of trained people, proven processes, and they have the tools that keep networks up and secure while giving

small businesses the ability to focus on their own businesses. They let you avoid making expensive investments in the people, hardware, and software needed to keep networks secure 24 hours a day, seven days a week and put it in their hands.

The problems are magnified in smaller companies because systems managers employed at smaller companies are often not as well trained and are less experienced than their counterparts in larger organizations and often, in very small organizations, systems management tasks are assigned to non-technical staff (Bassett, 2000). The typical systems manager at a small business also may be responsible for duties other than systems management (Bassett, 2000). Even companies with IT staffs are stretched thin, dangerously thin, in many cases. For years companies have had difficulties meeting all of their IT needs, let alone security. Letting an MSSP manage the security for a company as well as maintaining it's integrity will allow those companies to use internal IT personnel more strategically. Instead of fire-fighting network and security issues, the internal IT staff could be working on projects that are vital to your business and directly impact those companies bottom lines, such as ERP (enterprise resource plan) development, business applications, and e-commerce. Because MSSP's proactively plan, evaluate, maintain, and improve systems, networks, and security, the businesses experience less downtime, lose less productivity to network outages or security intrusions, and gain more time for your IT staff to work on projects important to your business. Also with most MSSP's being open 24x7 this gives small companies the piece of minds that their network is being watch continuously even though it's business hours may only be 8 to 5. Hackers do a lot of work overnight and without someone watching networks closely they do not know anything happened.

Many MSSP's are also MSP's (managed service providers) and can offer a small business a great cost effective alternative to hiring internal staff that has limited knowledge in all areas of computing. There are many people who know certain aspects of computers, but it is very rare to find a person who has all the skills to handle every aspect of a company's network security. MSSP's fix those issues by offering a company a group of people with various specialties all for a fixed rate each month, most times cheaper then hiring just one full time person for a year. When it comes to networks, the most time and resource intensive activity is the day-to-day network maintenance. Maintaining every component of a network can eat up the time and energy of even the biggest and most skilled IT staff. MSSP's take care of many security related issues such as maintenance of user accounts, firewalls, anti-virus systems, operating systems, mail systems, security updates, and backups. All of those are what keeps a company secure.

Summary

It is also understood that small businesses are the backbone of the economy: small businesses "represent 99% of all employers, employ 52% of all private workers, and provide 51% of the private sector output." (Bassett, 2000). Only time can tell what the future will hold for these companies, but everyone is aware that security will always be at the forefront of the computer industry. No network is ever completely secure and never will be, but there are many things companies can do to keep their network as secure as possible and protect those vital resources. Small businesses have a big challenge ahead of them to keep up on security without spending thousands of dollars to do so. They want to focus on their core business and have the ease of

mind that their network and infrastructure will always be up and secure without compromising of their data. If they follow put some effort in up front to secure their environment, put simple guidelines and policies in place to deal with their networks security, then they will be able to operate with the ease of mind that they are doing everything within their power to protect their company from the growing number of computer security threats.

References

Bassett, Greg, **Developing a Computer Security Proposal for Small Businesses - How to Start. August 8th, 2000.** URL: http://www.sans.org/infosecFAQ/policy/cssb.htm

Becker, David, Microsoft takes heat for Code Red. August 1st, 2001.
URL: http://news.zdnet.co.uk/story/0,,t276-s2092319,00.html

Feinberg, Joshua, Microsoft Exchange Server Backup and Restore: What You Don't Know CAN Really Hurt You. November 5th, 2001.
URL:http://www.smallbiztechtalk.com/news/archives/tips110501-bn1.htm

Feuer, Daniel, Reinke, Thomas, Protect your business computer from hackers. February 21st, 2000. URL:http://www.fireinternational.com/fire20000221.htm

Hall, Eric, Internet Firewall Essentials. November 15th, 1996.
URL: http://www.smallbizinfocentre.com/offsite.asp?ID=394

The Internet Economy Indicators. Facts and Figures. November 5th, 2001.
URL: http://www.internetindicators.com/facts.html

Luzadder, Dan, Corporate security gets urgent. November 2nd, 2001.
URL: http://www.zdnet.com.au/newstech/security/story/0,2000024985,20261636,00.htm

Sungard Planning Solutions. Regulatory Checklist.
URL: http://www.sungard.drexperts.com/knowledgenet/regulations.asp

Last Updated: May 27th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
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 Charlotte 2017	Charlotte, NC	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 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
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	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
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
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