Global Information Assurance Certification Paper

Understanding the Importance of and Implementing Internal Security Measures

GSEC Gold Certification

Author: Mike Durgin, mdurgin@synacksys.com

Adviser: Jeff Turner

Accepted: August 19th 2007

Outline

1. Abstract/Summary

Many Information Technology professionals concentrate on securing the perimeter of their network, ignoring the possibility of internal attacks. Internal security incidents can be much more costly than an attack from external incidents, and are more likely to succeed due to internal knowledge of the corporation. This paper will focus on the importance of internal security, types of incidents, motives, potential loss, and how to defend against them. It will show how many external incidents are successful due to inside knowledge of the organization, inside help, or are performed by insiders using the anonymity of the Internet.

The topic is relevant to the GSEC curriculum because it will discuss many threats, attacks, and countermeasures covered in the curriculum. It goes beyond what is taught as well because it will delve in depth into motives and real life scenarios to put the likely hood of an internal incident in perspective. Security professionals will want to read this paper because it will give a different point of view to threat origins, and that an expensive firewall or intrusion prevention system may not be the solution to all of their problems.

2. Introduction

Today, the news is littered with security incidents ranging from the latest worms and attacks to identity theft. Studies have shown that malicious code is at an all time high, mainly because of the profitability, along with the anonymity provided by the Internet.

As a result, many organizations are spending the majority of their security budget protecting their network against the various threats that are emerging on the Internet. They are purchasing expensive Firewalls, Intrusion Detection and Prevention Systems, as well as VPN devices to help mitigate these malicious activities. As a result, many organizations ignore the possibility of an internal threat. It is no surprise, considering the cost of many of the security devices out there, and the budget that organizations are given to work with. But is this the best way to defend your organization?

According to studies like the CSI/FBI Cyber Crime Report it is. Statistics over the years have shown that companies are reporting less and less attacks originating from inside the network. The Cyber Crime Report for 2003 shows the percentage of internal incidents reported to be steadily dropping, and 61% of the respondents in the 2006 report responded with internal revenue losses totaling less then 20% of their overall incidents. Looking at all of these attack trends and statistics, it is hard not to wonder how many of these incidents occur with help from an inside resources.

3. What is an Internal Incident

In order to secure and organization against internal incidents, it is important to understand what one is. An internal incident occurs when a resource inside of the organization is used in the attack. Examples could be anything from a resource accessed internally, an attack executed by an employee using the anonymity of the Internet to cover their tracks, to an outside entity that unknowingly factors into the execution of a security incident. It can even be an employee, contractor, or third party support technician who runs software or makes a change that has a negative impact on the organization. There

are so many examples that many security administrators neglect to even consider when securing an organization.

4. People within the Organization

One of the most often overlooked causes of internal incidents are people inside the organization. Whether it is a contractor who has signed a non-disclosure agreement, or an employee who has incentives to see the company do well, can they really be trusted? There are always cases where someone feels they were passed up for a deserved promotion, or are under paid. What about employees who have been fired or laid off? It is a common fear that people leaving a company may take clients, but what about people currently there? Many of these bitter workers may have intimate knowledge of the organization that could be damaging to the company's reputation, intellectual property, and financial status.

Often employers feel that employees working for the organization would maintain loyalty to their employer as they have too much too loose. But that did not stop Robert Hanssen, an FBI agent who sold secrets to the Soviet Union. Over 15 years he made 1.4 million dollars, roughly $90,000 a year. He committed treason, an act punishable by death for $90,000 a year. Considering the penalty for treason is execution, how many people would risk their life for $90,000 a year? It is amazing how quickly these penalties can be forgotten when the perpetrator has plenty of time to cover their tracks and a larger than life ego. Considering that the penalty is not as high in most cases, it is a very likely reality to be betrayed by a coworker.

5. Disgruntled Employees

Everyone always hears about disgruntled employees that leave feeling they were owed something, but most people feel the threat is neutralized once they leave the company. Painewebber, a large investment firm, knows this is not always true, thanks to Roger Duronio, who planted a logic

bomb that decimated their computer systems in 2002, that went off just a few weeks after he left the company. He anticipated his logic bomb would cause their stock to plummet, and purchased $21,000 put options, a security that make money if the stock goes down. Why did he do it? Because he felt he was not compensated enough for what he did. Often, workers can hear someone complain that they are not treated fairly, or have been passed up for a promotion in favor of someone less deserving. What is to say they will not seek retribution for how they feel they have been treated?

6. Corporate Espionage

Malicious intentions are not limited to ex-employees. Many workers may possess access to trade secrets that could be damaging should a competitor find out. In the past few years, both Duracell and Coca Cola have had employees steal secrets to sell to competitors. In both cases, the competitors did not solicit the perpetrators information and returned the information to the rightful owner while informing them of their employee's intentions. It is hard to imagine that competitors would always do the right thing and how often competitors solicit information they should not have.

In some cases, financial gains may not affect the competition, but be strictly for financial gain. In 2007, Fidelity National Information Services Inc. reported that a database administrator took records and sold them to direct marketing agencies. The records included names, dates of birth, addresses, bank account and credit card information. Imagine what that does to the company's reputation. Even with credit card protection programs, how many people will feel comfortable trusting companies that experience incidents like that with their business? It may be likely that the information was only used for marketing and any financial data was ignored, but how many people at the agencies that bought the information now have access?

7. Outsourced Personnel

What about crews that service devices like printers, copiers, and fax machines? Most people do

not realize that many of these devices have hard drives in them, which are used to temporarily store and reproduce the document. Anyone with a forensic background knows how easy it is to recover data that has been deleted from many forms of media. What would stop someone from stealing corporate information, or even steal identities using the information from previous transactions? What would stop someone from disconnecting the printer and plugging a laptop into the network? No one would raise an alarm, as a "technician" is working on the device that no longer works.

Most organizations employ outside help to take care of many daily tasks. It may be payroll processing, cleaning crews, hardware maintenance, and telecom companies, outside consultants, just to name a few. All of these areas are screaming for security incident to happen.

Outsourced personnel, whether they work on or off premises can open a large number of security problems. There have been many cases of companies that are blackmailed by these outsourced companies. Heartland Information Services, a company that outsourced medical files, had some of their overseas contractors in Bangalore threaten to release information if their financial demands were not met. The UCSF Medical Center also had an off shore contractor who felt she was owed money, and took the matter into her hands to use patient records as ransom to get what she felt she deserved.

8. User Ignorance

Frequently, naïve users can unintentionally cause a world of problems for an organization. They may not be aware of policies that are in place, and even though their activities may be legal, they do not understand how it can hurt company resources, as well as productivity.

How often is someone doing something without realizing their actions could be harmful to an organization? Whether it is software they are running that is not part of a standard build image, sites they are surfing that could be considered offensive, or legally owned copyrighted material that is unknowingly available to people who have no right to use the material.

Users should be prohibited from accessing non-work related media at work, such as streaming video and audio. Multiple users accessing these types of media can cripple a network in a matter of seconds, as happened to a multitude of companies during 9-11 when the majority of the users went to http://www.cnn.com to view the videos of the planes crashing into the World Trade Center. Web caching devices can help limit frequently accessed sites from clogging the outbound bandwidth.

Many users have gotten hooked on Peer to Peer software, downloading legal and illegal media and software. Many also work in an environment that has much more bandwidth available to them when compared to their home ISP, which can cause a person to use their work computer to download these files. This raises a number of issues with users downloading large media files from these peer to peer networks, they will use a lot of bandwidth, which could degrade and even halt the network.

Much of the media on the Internet is copyrighted material. Even if the user downloading the material owns a legitimate copy, and they feel that justifies why they can have it on their computer, there are likely still plenty of ways for others to copy these files that they do not have right to. Any illegal copies of music, movies, and software present on a system can be a liability to any organization.

Instant Messaging is another large issue. It is an insecure communication method, which in most cases, sends all messages through a third party server. Any server that the message passes through in transit can read whatever information is in the messages. How many users are aware that these clear text transmissions are readable by anyone with access to a system it touches? Email falls prey to the same problems as well. Policies need to be in place about use of email and instant messaging specifically for this reason. Internal instant messaging proxies or servers may be recommended to allow it to be used for work related purposes, as well as encryption methods for both email and instant messaging like PGP.

Administrative rights to workstations can be problematic as well. Aside from the potential of installing a virus on their system, users may try and download software flagged by Anti-virus

applications for other legitimate reasons, but the user can just turn off their security software to get around this. It also creates problems for Desktop support teams to trouble shoot since it is not part of a standard build. Users need to only be allowed rights to do their job on their systems.

Many of these issues can be mitigated by having well defined policies in place, as well as educating users so they can see why they are important. Users need to show they understand them as well as any addendums after they are hired, and can be held accountable for breaking them. Signed forms stating they understand the policies are a must if a company ever wants to enforce them or defend them during litigation. Policy changes after an employee is hired also must be acknowledged by the users in the same fashion. Many organizations are guilty of using subcontractors, and not putting them through the policy training the full time employees do. If a subcontractor creates a "hostile" work environment, would the company be able to absolve all responsibility because they were not an employee?

9. Social Engineering

The biggest security threat has, and always will be the human factor. Because it is in our nature to trust what we see and hear, many potential intruders try and play on this trust. Many attackers use social engineering, a non-technical attack that takes advantage of our naive and trusting nature. It can take many forms, including shoulder surfing while someone enters a password, tailing in to a secure facility without proper identification after convincing an authorized person they should be let in. It can even include mail that tries to harvest information.

Think of the number of people who have access to an organization's headquarters. Aside from coworkers with vendettas or personal agendas, many third party personnel, like cleaning crews may have access after hours. They may not have motive, but they also may not have much loyalty either. Anyone who might be willing to pay them could get easy access to resources readily available.

Association for Competitive Technology found out how close their cleaning crew could have come to giving out potential information. A woman who went by the name of Bianca Lopez unsuccessfully tried to bribe their cleaning crew after hours for garbage, offering them anywhere from fifty to five hundred dollars, attempting to win them over by speaking in their native language. She offered five hundred dollars just for garbage that could potentially have no information. The two instances were unsuccessful, but no one knows if they were the only attempts, and if any other attempts were successful.

Often, people leave important information on their desk, in plain sight of anyone who walks by. Any network maps, business cards, notebooks can be used to launch an attack. If a firewall had a vendor's business card tacked to a board in their cube, what would stop someone from calling with that information and saying, "This is Jim, your Acme Firewall representative. We just had a major vulnerability released with Firewall version 1.2.3. Would that affect you"?

The Firewall administrator may trust the phone call and say, "We aren't vulnerable, we are running version 1.2.5". Now, an attacker has the version of the firewall running and can look specifically for vulnerabilities against that firewall, all because a business card was left in plain sight.

People will also rely on fear to get things done. Often, people may use the name of a high powered business executive, and call the help desk to get "their" password reset. Some times they may even threaten serious consequences if their demands are not met. Employees need to be aware that this type of attempt to usurp power is in fact a likely attempt for someone else to gain access, even if the call comes from a number in the work facility.

In some cases, people may spoof email, or even send email from an anonymous account made to look like a legitimate company email. A common example may involve sending an email from the "Support Team" claiming that if your user name is on a specific list in a document, that you must change your password. Meanwhile, the document could be loaded with a virus that compromised the

users system, giving full access to the attacker without even responding to the message.

Today, portable devices that can be connected to a computer using USB or 1394 interfaces pose serious threats, and not just as a device to steal sensitive information with. Steve Stasiukonis, founder of Secure Network Technologies Inc., performed an audit on a credit union concerned about the dangers of devices like USB thumb drives, iPODs, and other similar storage devices. He took 20 USB thumb drives he had gotten from vendors and conferences, stored a malicious image he crafted on them, and left them in various places, like the parking lot, smoking areas, and other easily accessed areas of the facility that the employees frequented. After 3 days, 15 were found by employees that viewed the image. This can be tough to avoid, but user education is a must in this area, as well as policies prohibiting external hardware from being plugged into a computer. As operating systems evolve, it is likely that most will give administrators the ability to disable the USB ports, but it is not uncommon for Administrators who worry about this to cover the USB ports with hot glue as a defense. Before even considering something like that, be sure to check with your manufactures support, which potentially could be voided.

Another reason these attacks are so successful is because many people know more then their job requires. Do system administrators need to know what kind of firewall they are running? Does a developer need to know where intrusion detection systems are located? Does everyone need to know how the security logs are audited, how often video surveillance is reviewed, or that the card readers and palm scanners used to enter secure rooms do not keep a log? Giving out only enough information for an employee or contractor to do their job is a must.

10. Physical Security

Another issue is physical security. Your information is only as secure as the door to your facilities. It is not very hard for someone to take physical devices if the door to the room it is stored in is not secured. If there is a card reader system, it is easy to use someone else card to gain access. Why

wouldn't someone say to a co-worker, "I'm going to lunch. I left my card home, can I borrow your badge to get back in the building." Now they have full access to every resource that person had, and are leaving an incorrect audit trail.

Many companies use identification badges to enter their facilities. While this is an excellent practice in physical security, often, the information on the badges are overlooked, until they fall into the wrong hands. While they need to include something that makes them distinguishable against other badges, they should not show anything that indicates the company the employee works for, the location, or even the employee's name. Any of these can help allow the person who finds the card a way to locate the facility it can be used at, and use it or a forgery to try and enter the facility, as well as give them an identity to use in a social engineering attempt. Even numbers listed to call to return a lost card can be used for this as well. Forcing employees to notify your security team as soon as they realize they do not have it so the badge can be disabled is the best defense against lost cards rather then having identifiable information on the card.

Other issues are not thoroughly testing physical security measures. Again an audit performed by Steve Stasiukonis shows us unique flaws in common security methods. In his audit, he walked up to a card reader required to gain access into the building with the intent of trying every magnetic card in his wallet to get in. The first card he tried, a grocery store shopping card, allowed him to get inside. On top of it, he managed to get some scrubs which, dressed as many of the other employees, made him look as if he was a legitimate employee. Within minutes, he was able to even locate a desk with post-it notes containing user names, passwords, and in some cases detailed descriptions as to what they were used for.

Obviously, there was a miss-configuration on the card reader, which would have been spotted if it had properly been audited. On top of that, no one questioned why they should be there. It is critical to thoroughly examine the physical security in place, test it to ensure it works, and enforce that all personnel have proper identification visible. Even letting someone tail in with a legitimate badge is ill-

advised, as people may be able to get a misplaced badge and create a forgery. Two factor authentication is a huge benefit in these instances.

11. Password Security

In addition, this example shows that password security is usually not considered very important by most users, despite how costly it can be to an organization. In many cases, people may ask for a password to trouble shoot an issue. There is no reason why any password should ever be given out, or written down, making it easy to retreive, even when stored in a place the user deems secure like a wallet or purse. All passwords are generated with an personal algorithm of some sort. Whether it is something insecure like a pet's name, or something strong like the first letter of a known phrase with some character substitutions, the person with the password now has insight into the password generation scheme that was used. And if that password is used anywhere else, the malicious person may not have a hard time figuring out what else they can access with it.

Proper policies should be in place to make sure a password is at least 8 characters long, as well as requirements for upper and lowercase letters, numbers, and special characters to be used. Policies should not be so strict, otherwise user will write down their password. They should also be limited to how often they can change their password, otherwise, if password history stores the last 10 passwords, all they have to do is change their password 10 times in order to reuse their old password.

12. Conclusion

While the human factor can be the hardest incident to prevent, it can be a cheap one to mitigate. Users must be continually educated to these types of threats. They must be aware of policies, have records stating they understand the policies, and know they are accountable for their actions. In any penetration tests done, it is imperative to include social engineering in the attack simulations.

Security is important in all aspects of an organization. Neglecting any one area can be devastating to an organization, as has been shown by some of these real life examples. The importance of securing an organization internally should never be overlooked. Security is only as good as the weakest link in an organization, so be sure to examine all possibilities carefully when doing your risk assessments and budget planning.

Education, well defined policies, physical security and audits can be help immensely when trying to secure an organization against internal threats. Calling users or groups and trying to get them to give you a password is free, and effective, as is trying to walk in without using proper identification. Documenting all of these issues, and making sure employees know that they must adhere to these policies.

13. References

(2004). "Computer Crime and Survey 2003". CSI/FBI.
Retrieved August, 8, 2007 from
http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf

(2007). "Computer Crime and Survey 2006". CSI/FBI.
Retrieved August, 8, 2007 from
http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf

(December 17, 2002). "Disgruntled UBS PaineWebber Employee Charged with Allegedly Unleashing 'Logic Bomb' on Company Computers". United States Department of Justice.
Retrieved August, 8, 2007 from
http://www.usdoj.gov/criminal/cybercrime/duronioIndict.htm

Brenner, Bruce. (July 5, 2007). "Malicious insider sells Fidelity National customer data". Searchsecurity.com.
Retrieved August, 8, 2007 from
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1263233,00.html

"§ 2381. Treason". Cornell University Law School.
Retrieved August, 8, 2007 from
http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002381----000-.html

Associated Press. (March 13, 2007). "Your New ID-Theft Worry? Photocopiers". Microsoft Certified Professional Magazine Online.
Retrieved August, 8, 2007 from

http://mcpmag.com/news/article.asp?EditorialsID=1236

Hines, Matt. (March 18, 2007). "Duracell IP thief sentenced". InfoWorld. Retrieved August, 8, 2007 from http://weblog.infoworld.com/techwatch/archives/011958.html

Lazarus, David. (April 2, 2004). "Extortion threat to patients' records Clients not informed of India staff's breach". San Francisco Chronicle. Retrieved August, 8, 2007 from http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2004/04/02/MNGI75VIEB1.DTL

Stasiukonis, Steve. (June 7, 2006). "Social Engineering, the USB Way". Dark Reading. Retrieved August, 8, 2007, from http://www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1

Stasiukonis, Steve (July 19, 2006) "Social Engineering, the Shoppers' Way", Dark Reading http://www.darkreading.com/document.asp?doc_id=99347

Last Updated: May 28th, 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 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	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	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