Internal Threats – A personal experience
V1.4
By Christopher M Hill

Abstract

In 1998, Louis J. Freeh, director of the FBI, said in a brief delivered to Congress while discussing National Security computer related incidents said, “The most imminent threat today comes from insiders” (Freeh, 1). Also, in 1998, the FBI investigated me as a disgruntled employee for allegedly entering my previous employers systems in 1997 without authorized permission. The knowledge gained with this experience taught me basic computer security principals. The questions and answers that were given to my previous employer, my ISP, my new employer, and myself opened my eyes to why it is important to be cautious when dealing with access control, security policy, intrusion detection, vulnerability assessment, and auditing, especially from the inside. Security Industry Experts suggest that employees steal data “because of dissatisfaction with salary, promotion opportunities, or working conditions; conflict with managers or financial problems linked to alcohol or drug use”. (Unknown, 2) The numbers released by the FBI on Internal hacks and the damaged caused by these disgruntled employees proves that a company must carefully plan its strategy for dealing with Internal Threats. The FBI states that, “The Computer Security Institute documented the statistics in a reported study on computer breaches. This year's survey of 538 respondents found 85 percent experiencing computer intrusions, with 64 percent serious enough to cause financial losses. Estimated losses from those willing to provide the information tallied $378 million, a 43 percent increase for the previous year”. (Unknown, 3) The FBI also states that, “71% of respondents detected unauthorized access to systems by insiders”. (Gonzalez, 4) My former employer did not take these numbers seriously and due to that fact suffered a devastating attack that crippled his network for 2 days. This paper is designed to step through the alleged attack and how my previous employer could have prevented this attack by taking appropriate actions following my resignation, and what he should have done after the attack to catch the real hacker and ensure that the vulnerability was never exploited again. This paper is designed to step through this hack that I was accused of committing, discuss the details of the attack, and how the attack could have been prevented.

My Company History

The company was a medium-sized ISP start-up based in North Carolina. I was hired as the first employee and was responsible for all network, user, software, and customer administration. The company hired about 15 employees in the first 3 months. I had complete knowledge of all systems, users, networks, and software installed on every machine and device on the network. I had implemented RADIUS as the authentication method for our customers to access the Internet. The Router was configured with an access control list to allow only access to certain ports to the Internal Network and that users could only access the internet and local services provided to them. Windows NT was locked down with NTFS so that only certain files and folders could be accessed by the outside world. This included ftp, web, email, and newsgroups. The ftp servers were locked down with proprietary ftp software, as well as the email servers (post. office), and the newsgroup server. All Windows Servers were up to date on patches and secured to the best of my ability only using native tools to the OS and Application. This was a good start but more had to be done to insure a solid security foundation.

I discussed with my manager several times about computer and security policies that should be implemented, but he did not think that we needed one being such a relatively small company. This was a big mistake because security policies produce guidelines that must be adhered to, not just by employees but also our customers. This could have saved him the headaches he encountered later when his system where compromised.

I also made recommendations to my boss about the implementation of Firewall, VA, IDS, and the analysis aspect of security and what items we should put in place to insure tighter security over our sensitive information in the company. Even though cost was not an issue he was not receptive to my suggestions because he felt it may hinder end users from accessing the internet through our network. Basically, I guess I didn't do a good job of selling him on what he needed, or he just wasn't listening.

My compensation was based upon the number of users that the company acquired over the first 1500 customers. Unfortunately, after one year the agreement that was reached during our employment negotiations fell through, I personally felt that I needed to make a change. I opted for a move to Atlanta and a consulting position.

The company was in disarray after my departure. Two months after I left the company I was contacted to dial in and help them with a server crash. I obliged and helped them straighten out some issues that were plaguing their servers. This happened several more times over the next couple of months. I worked with them over the phone to resolve downed servers. A new network administrator took control of the servers on May 15th.

The Incident

The incident occurred almost 3 months after I had left the company in June. I was called by Tech Support about a Livingston portmaster that was not allowing people to login. I asked where the new administrator was and what he was doing about the problem. He was out and no one could locate him. I dialed into their system and reset the portmaster. This knocked off about 10 people who where logged on but allowed for the other 20 ports to be useable. That same day I recognized that some of the Web Pages that I had written and placed for customers where either removed or had my name removed from them. I called and asked that my pages and my name restored unless the page was removed for lack of customer payment. I accessed the servers and restored my company name to the pages that my name had been removed. I had a contract agreement that my company name would be left on pages developed by me, and that I had access to those web pages at all times. Two days later I called to talk to one of the tech support people and was informed that the servers and routers had crashed and that they had contacted the FBI to investigate. Three months later an FBI agent questioned me at my resident concerning the alleged incident. This caused me grave concern. I had been accused of accessing the company's computers without authorized permission.

The hack involved the use of other employee's UserID's and password. The hacker also dial-ed in to the company through a modem which gave the hacker an IP address on their network. The attack was designed to disable all accounts but one while changing the UserID and password on that account for future access. All log files where deleted and all access was denied to internal employee's. A list of UserID's were stolen and a customer list from the radius file with all customer access codes were stolen,

The Accusations

The FBI accused me of hacking into the company's servers and destroying company data, changing administrator passwords, and setting up backdoors for future access. I was investigated and questioned over a 3 month period, but was never brought to trial. These accusations were not provable because there were no policies, auditing, or restrictions set in place to govern former employees. This paper is a detailed account of how my employer could have prevented these attacks on the systems and successfully prosecuted the perpetrator for any damages that might have been caused by a successful attack.

Lesson 1-Being Prepared

The first step to ensure a secure network in a new organization is to develop a working policy that can grow as the organization becomes larger. A policy enables the employer the ability to lay out certain expectations of employees in document format, and also give specific instruction to an employee not to tamper with company related documents after they have resigned or are released from the company. This is also true for people who access a company's Network through illegal means. These policies are contracts with the employees so that they understand their roles and obligations to the company. Three types of policies should be implemented to create an effective balance for the entire organization (Unknown, 5). A Program Policy is important to set a high level policy that forms the basis for your entire company's security policy from a high level. Issue-Specific policy describes how personnel should handle certain situations, such as Internet usage, mail usage, and employee removal from an HR database. A simple policy such as the one for the University of Arkansas Medical School (Unknown, 6) illustrates the ability to assign responsibility to a group of users to take away granted rights to terminated users. The final type of policy is a system specific policy that outlines the use of specific machines with special functionality on the network. Policies should be simple and easy to read. Employees should read and sign a copy and that document should be filed in case of an employee or former employee breach. Hewlett-Packard suggests on their security web site that, "A sound security policy should begin with working with your human resources team to include a discussion of security with new hires. From day one, employees should be well-versed in everyday security policies, such as rotating and protecting passwords, carefully handling e-mail attachments, regularly backing up valuable company information and the like". (Unknown, 7) This will allow law enforcement personnel to determine the boundaries in which an employee should be operating.

Policies also make it easier for law enforcement officers to determine if an employee or former employee has access a system illegally. A policy is considered a binding agreement between the employer and employee. If broken the employee may be libel for any damages and also may have criminal action taken against him or her. A policy must be explicit to work properly. There should not be any section that can be left to interpretation, and all policies should be approved by a lawyer.

So how do policies affect my case? Had my previous employer used policies then a few things would not have happened. First, if a password specific policy had been in effect, then a former employee would not have permission to use other employees UserID's, backdoor UserID's, and passwords to login. The password policy would have ensured that at the most a former employee would have a specified number of days to access the system before any backdoor UserID's and passwords would have their password changed or locked out. Second, a policy related to the access of systems would have spelled out what access a user should have to the former employee. Any notion that a former employee may have about access to these systems would have been dispelled by a properly placed system policy. Third, there was no policy in effect, and my former employer had allowed me access to his systems with his knowledge. Having a trusted former employee help fix a problem is okay, but there must be some accountability put into place to keep that former employee from gaining complete access to everything. My former employer should have had me sign a contract stating that I will adhere to certain guidelines or policies when accessing his systems.

Auditing

There were also no auditing set on the machines so the information that was collected was very minimal. It is important to understand what needs to be audited and to make sure that there is an accompanying auditing policy. Understanding the chosen operating system and the information that can be collected is important in catching unwanted access to pertinent information. This information should be collected, stored, correlated, and reported on so that a company can maintain an acceptable level of security. There are products on the market that will do this and do this well. My former employer did not understand the importance of operating system, application, and hardware auditing. The information gathered just from the basic auditing of information could have been enough to implicate a simple hacker with limited ability. If the incident was enough to contact the FBI, then it should be stated that any audit information given to them would help them locate and specify important information on the hack.

The auditing should have been set to at a minimum capture Logon/Logoff failures and successes, file access success and failure, security policy success and failure, restart and shutdown success and failure, and audit account logon events on the Domain controller only. This would have given my former employer decent information on what had been happening to his systems.

Lastly, and in my opinion the most important thing when dealing with a former employee who has in-depth knowledge of your systems. Know what you're up against. If your former employee is Sally in HR then you can be reasonably sure that she will not gain access through a deceptive manner, however, if it's Chris who is a network god and could do anything then it is time to worry. A company must realize the difference between a minimal security risk and definitive security risk. I think had my former employer taken the time to ensure that all personnel with an administrator account had changed their password and all other administrator accounts disabled then he would not have had to worry about a former employee accessing his system by simply knowing a UserID and password of another employee. There has to be a plan for keeping administrators accountable for their access. I ran into a good plan on the SANS website. This plan outlined how a company could use multiple access control products to help thwart administrative abuse. The plan calls for a tool to "funnel information through a single point", a "SecureID token-based authentication which provided and additional level of authentication", and some "freeware tools to ensure that a machine logs off if not being used in a reasonable amount of time". These changes would have helped my employer keep an employee or former employee with administrative right from access these systems unannounced. This is important because "Administrative access to critical infrastructure is one of the most neglected areas of security" (Thurman, 8). Also, running simple reports from marketplace administration products on a daily, weekly, and monthly basis would insure that personnel are changing their passwords on a regular basis and that administrators are not making it so their password never expires. This is a simple policy that could have made it harder for the former employee to gain access, but important enough to have been inserted into a company policy.

Lesson 2-Identification of a Problem

Identification of an incident beforehand can help insure that there is awareness of a potential problem before it happens. People tend to be reactive rather than proactive in finding out issues. Companies have long sought to be proactive in the systems monitoring space, but have failed to realize the importance of being proactive in the security arena. Identification takes shape with tools that can analyze systems and correlate information to display a view of what is accessing a network. A security administrator must be able to be proactive by receiving accurate information from data provided by Intrusion Detection Systems. Identification of a problem is next to impossible without certain tools to help you discover who, what, when, and where. Identification of a problem should be assigned to an incident handler. This handler must identify the problem and analyze it to ensure that incident is not a false positive. Once it has been determined that there has been a breach, someone must develop a plan to gather and store all evidence pertinent to the attack. This will allow for a better understanding of the incident for future knowledge and supply law enforcement with information that can be investigated.

My employer simply did not have the proper tools installed to catch someone accessing their systems. Had there been a Host-Based Intrusion Detection Tool (HIDS) in place there could have been consolidation and alerting based on events. These events could have been saved to a database and stored for future forensics. However, not having a HIDS in place the chance of having the event log overwrite or erase this pertinent data is exponentially greater. A simple event log consolidation tool would have helped the FBI investigate certain events that could have given them clues to any mischief on the machine. Failed logins, administrative logins, or employee logins at odd times could have helped with knowing what happened on the machine. Monitoring User Behavior on the machines is important to understanding the various ways a machine can be breached. Simple OS auditing on the machine would have also provided important information to the company. My employer tried to use log files that just did not contain enough information to understand exactly who or what had access and changed his systems. He needed an Intrusion Detection tool that could detect, alert, and correlated security information in real time.

A policy governing all IDS systems is a very integral part of the equation. Every aspect of the IDS systems should be specific to who administers the system, who monitors the system, who can receive information to the system, and who can not access the IDS system. In the military we had a saying that basically stated that bad planning led to bad procedure. This is true with every implemented product in an enterprise. A deeply thought out plan implemented to near perfection can thwart trouble most of the time.

I found a good example of a company using an Intrusion Detection System to determine employee behavior. An article in Network Magazine outlined how Sony Entertainment uses IDS to control access to their network. The article describes in detail an anomaly based IDS system that correlates and discovers weird changes to the network. Jeff Uslan, director of information protection and security, says that, "If there is something weird on the network, the IDS gives me the opportunity to see where it's coming from – what network, what segment, what computer system. It gives me a few minutes or an hour to get ahead of the problem." Uslan goes on to describe how he uses the system to help figure out "the myriad of unknowns swirling inside and outside his network". (Conry-Murray, 9) This is important because a properly run IDS system could have helped my employer detect a wide range of anomalies that went undetected by not having some type of IDS system in place.

There should have also been a vulnerability test on all machines. Producing reports on weak passwords, or system related vulnerabilities based on CVE standards, would have provided my former employer with system weakness that could have been fixed by patching. My employer should have it mandated in his security policy that assessments of every system are done at certain intervals that would produce an understanding of what holes he has on his network, yet allow for minimal network usage and system downtime. This may have helped him in identifying problems before a hole on a system could have been exploited.

Lesson #3 -- Containing the problem.

The systems where maintained online for 2 days while my employer tried everything possible to get back into the machine. He also did not do any forensics or save off any data pertaining to the machines. This allowed the hacker to come in and delete certain log files that may have held pertinent information concerning the hack. Even with the basic logging some information might have been saved to give the FBI, unfortunately because of his lack of knowledge what could have been saved was lost.

Once the breach had occurred my former employer should have contained the attack and backups should have been made immediately. The fact that the systems could not be logged onto should have told my former employer to pull the plug on the affected systems. Having done so, no further damage could occur and any evidence left behind might be saved. This also would have prevented the hacker from going back into the systems and looking for evidence to erase or other things to steal. My former employer should have then gotten off all log files that could contain evidence for later analysis. He should have also saved the router log files off so that they could be examined and cross-referenced to the logs off of the attacked computer systems. Now that all pertinent information has been removed, my former employer can now restore his systems.

The system should have been ghosted at a timed interval and it should have been determined which ghost image was no compromised. Had there been a ghosted image my former employer could have had his machines back on-line in no time, and had a backup of the failed system.

Lesson #4 Recovery and Understanding

My former employer should have gathered this information and then developed a strategy to eradicate and recover from the incident. First, he should have evaluated his defense and determined what caused the problem. Knowing the root cause allows for him to get specific on the types of information that he is looking to find in his stored data. Second, the company should have evaluated the backup code to make sure that it wasn't corrupted. He had a problem so the best thing to do was to look at his systems individually and make sure that there were no vulnerabilities that the hacker could exploit. Once this was done and the restore was complete my former employer should have wasted no time monitoring his servers for other hackers who may have heard of the "easy access" to his servers and might be contemplating the same hack. If a monitoring system is in place that can correlate and separate information my former employer would have a better chance of catching the hacker if he further tries to hack into the network.

Lesson #5 Follow-up and Review

Once the hack had occurred and everything was back to normal with some new policies and products in place to help with security, my former employer should have developed a report on the incident. He should have gathered information from every employee who was involved and put together a detailed report so that lessons could have been learned from the incident. Once the proper employees were briefed and recommendations were made everyone should have been aware of what they did to contribute to the problem. Then they should have been rewarded for the hard work they did on solving the problem. Recommendations should have been made so that everyone understands what is expected of them, and the security policy should have been updated and signed so that everyone has a responsibility to keep the company safe. This would have ensured that everyone is on the same page and working together to ensure the safety of the company.

My employer then should have embarked on a plan to educate his employees on security techniques. Training these employees would have given him an edge by having every employee from the system administrator to the accountant become aware of what they can do to prevent access from others trying to use their computer or password to access the company's systems. A company must have some trust in their employees, but access to sensitive must be examined often to ensure that no one but authorized personnel can gain access to the data.

Finally, it is important to understand that if a hacker or insider is determined enough they will gain access to data. It is important to make that access as difficult as possible, and to try and make it so that if someone illegally access critical data that there is enough information to catch the perpetrator.

In Conclusion

My former employer made major mistakes by underestimating the potential strength of hackers on the internet, internal employees, and overestimating the security that he had in place. A proper policy put into place early would have ensured that the proper security measures surrounding the network was implemented and maintained. The policy would have forced users and administrators to do the simple security tasks such as password change, backup of logs, and what to do when an employee leaves a company that can have a great effect on the overall security of a network. It is important to recognize that there were not any real security tools in place to look for vulnerabilities, intrusion detection, TCPWrappers, alerting tools, or any analysis tools to take information from routers, firewalls, and server to look for events that could be correlated and acted upon. These tools are a must in any network to determine if any breach has occurred and to give the security professional the ability to try and track down and understand the security incident. Once these security tools are in place my former employer would have had the ability to take that information gathered and determine what happened and would have had the ability to help the FBI with their investigation. However, with the network in the state that it was in and the improper decisions that were made there was very little valuable information given to the FBI to track down the intruder. The forensics needed in prosecution dictated that my former employer supply the FBI with detailed information of the attack. This could not be accomplished because there was not information to give due to the fact that there were no policies, no auditing, no IDS, no vulnerability assessment, and no analysis of the collect information. My former employer did not have any information to give to the FBI surrounding the attack because he had no software in place to keep unwanted people from accessing his network, software to store and analyze information on the attack, and ways to have this information alert employees to potential problems. He did not properly plan an effective security solution for his environment. If he had done so he would not have had the hack on his network, or he probably would have given the FBI enough information to catch the person who did hack his network.

Now, the question you have been asking yourself since the first paragraph. Did I do it? Of course not!

References

1. Freeh, Louis J. “Statement for the Record of Louis J. Freeh, Director Federal Bureau of Investigation on Threats to U. S. National Security Before the Senate Select Committee on Intelligence Washington, D.C.” , FBI Website, January 28, 1998, http://www.fbi.gov/congress/congress98/threats.htm
2. “FBI Sting Operation Thwarts Disgruntled Employee's Attempt At Corporate Espionage & Suspect Is Arrested”**,** Vector Networks, January 22, 2002, http://www.vector-networks.com/press/general01-02.htm
3. Reprinted from American Society of Industrial Security, “FBI Sting Operation Thwarts Disgruntled Employee's Attempt At Corporate Espionage & Suspect Is Arrested”**,** Vector Networks, January 22, 2002, http://www.vector-networks.com/press/general01-02.htm
4. Gonzalez, Guadalupe. “Statement for the Record of Guadalupe Gonzalez Special Agent In Charge, Phoenix Field Division Federal Bureau of Investigation on Cyber crime”, FBI Website, April 21, 2000, http://www.fbi.gov/congress/congress00/gonza042100.htm
5. SANS training Manual, Security Essentials, volume 1.2 page 2-4.
6. “Terminated Employee Access Procedure”, University of Arkansas Medical School, June 01, 2000.
7. “Firewalls: the tip of the security iceberg”, Hewlett-Packard Corporation, October 1, 2001, http://www.hp.com/large/news/security/oct01_e.html
8. Thurman, Mathias. “An effort to restrict access to a company's production servers has unintended consequences”, Security Managers Journal, SANS Organization, April 23, 2001. http://www.sans.org/newlook/resources/SMJ/042301.htm
9. Conry-Murray, Andrew. “Sony Pictures Casts Intrusion Detection in Starring Role for Network Security”, Network World, Volume 17, Number 7, July 2002.