3-1-2008

Insider Threats to Information Systems

James S. Griffin
Air Force Institute of Technology, James.Griffin@afit.edu

Michael R. Grimaila
Air Force Institute of Technology

INSIDER THREATS TO INFORMATION SYSTEMS

James S. Griffin
Air Force Institute of Technology
James.Griffin@afit.edu

Michael.Grimaila@afit.edu
Center for Cyberspace Research
Air Force Institute of Technology
Michael.Grimaila@afit.edu

ABSTRACT

There are few, if any, organizations immune to the adverse and costly effects of successful information system attacks. As reliance on information systems continues to increase, organizations must continue to implement effective computer security measures to maintain their operability. This paper focuses on internal attacks executed by those individuals within the organization who have authorized access to information systems and behave in an unethical manner. We examine categorization of insiders; the motives and psychological profiles behind their destructive behavior; and conclude with a discussion of several measures that organizations can implement in order to detect and defend against insider threats.

Keywords

Insider attacks, insider motives, defensive measures

INTRODUCTION

Over the last three decades, information systems have gained a more prominent role in organizations. Information systems have become a critical component within organizations and are integral to their ability to operate effectively and efficiently. As businesses continue to increase their reliance on these information systems, they become more dependent on them. This dependency creates vulnerabilities, which leads to threats that become an ever growing concern. According to Jajaodia, Ammann, and McCollum, (1999) "an information warfare attacker's goal is to damage an organization by disrupting its information systems" (p. 57). Cyber hackers have increased in numbers, which coincides with the increasing ease in the ability to disrupt a business's operations by utilizing prepackaged computer hacking tools, kits, and programs readily found and on-line. Both external and internal threats continue to present security issues for organizations. Specifically, insider threats have increased over the years and continue to negatively impact operations. Organizations must understand insider threats and the risks and hazards they present, recognize their vulnerabilities, comprehend the different types of potential insider threats, gain insight into the reasons behind employees' attacks on information systems, detect those attacks, and implement countermeasures to defend against them.

INSIDER THREAT DEFINED

The 2006 Computer Security Institute / Federal Bureau of Investigation (CSI/FBI) Computer Crime and Security Survey identified thirteen categories of attacks that organizations are exposed to, with viruses, laptop/mobile theft, insider abuse of Net access, and unauthorized access to information topping the list and representing a majority of the incidents reported by those organizations (Gordon, Loeb, Lucyshyn, & Richardson, 2006). Of those thirteen types of incidents, a significant number of them are most likely implemented by insiders. Fortunately, though, the survey data indicated that 61 percent of the organizations who responded believed that insider threats accounted for less than 20 percent of their cyber losses. This indicates that more attacks come externally to an organization than from within. So, what are those internal threats?

Literature provides numerous definitions for insider threats or insider attacks. Schultz (2002) defines an insider attack as a "deliberate misuse by those who are authorized to use computers and networks" (p. 526). Theoharidou, Kokolakis, Karyda, and Kiountouzis (2005) define an insider threat as "threats originating from people who have been given access rights to an IS and misuse their privileges, thus violating the IS security policy of the organization" (p. 473). Stanton, Stam, Mastrangelo, and Jolton (2004) define insider threats as "intentionally disruptive, unethical, or illegal behavior enacted by individuals who possess substantial internal access to the organization's information assets" (p. 2). Finally, White, Fisch, and Pooch (1996) consider insider threats as those "in which the threat of an attack or damage comes from someone inside the organization" (p. 16). Each of these definitions involves three critical components: (1) individuals within the organization (2) with authorized access to information systems (3) who behave unethically.

As discussed by Hayden (1999), insiders are employees, contractors, service providers, or any worker who have rightful access to the network or information systems. As an individual's access to and knowledge of the organization's information system increase, the potential threat of misuse increases. Thus, the organization is presented with the greatest risk by this individual. Similarly, Nguyen and Reiher (2003) attribute the largest threat to computer security to insiders because of their intimate knowledge of the organization's business and computer network structure, to their access to information systems, and to their trust instilled in them. Shaw, Ruby, and Post (1998), in agreement, cite that employees, with their positions of trust placed on them that would hopefully translate into trust in their desire to promote the business efficiency, present the greatest risk of damage to information systems. These factors combine to create an extreme vulnerability within the organization, both to their information systems and to their bottom line. Finally, Tipton and Krause (2001) estimate that one in every 700 employees is working against their organization's interests.

FISCAL IMPACTS TO ORGANIZATIONS

Organizations are primarily concerned about internal and external threats because of the potential fiscal losses experienced following successful attacks. Of the 313 respondents in the CSI/FBI survey, an estimated $52 million was lost due to both internal and external attacks on organizations (Gordon et al., 2006). This is a markedly sharp drop from 2005, when over $130 million was reported lost due to attacks from 639 respondents. The drop could simply have occurred due to the lower number of respondents providing data; however, in 2006, the average loss per respondent was $168,000 versus $204,000 in 2005. Despite these relatively low numbers, they are very misleading. The fiscal losses reported only include those organizations that actually responded to the survey and, more importantly, were actually able to calculate the monetary loss to the organization. The true fiscal losses to all organizations throughout the United States and around the world are unimaginable.

The CSI/FBI survey indicates that internal losses alone range between $10 million to $20 million to those respondents (Gordon et al., 2006). This large range resulted from organizations not knowing exactly where the attack originated from, but most likely internally within the organizations. These categories include unauthorized access to information, laptop or mobile hardware theft, insider abuse of Net access or e-mail, abuse of wireless network, instant messaging misuse, and sabotage of data or networks. It must be noted again that these numbers represent only the organizations that reported attacks and could attach some form of financial loss to the incident. Those unreported or unrealized insider attacks contribute to significantly more losses. Additionally, as Shaw et al. (1998) point out, insider attacks are more successful than outside attacks, and as a result, contribute to significantly larger financial costs to the organization.

CATEGORIZATION OF INSIDERS

Existing literature identifies several categories of insiders using various names. For example, Hayden (1999) specified four categories of insiders: traitor, zealot, browser, and well intentioned. Traitors involve those individuals who have malicious intent behind their actions and a desire to severely impact their organization's operations. Individuals classified as zealots feel very strongly about their stance and do not agree with their organization's position on certain issues or subjects. Zealots attempt to expose their organization to the public by releasing information to outsiders or by granting access to outsiders in an effort to reform the organization. Browsers, on the other hand, represent those who are overtly curious about information that they are not granted access to and obtain or review data not intended for them. Finally, well-intentioned individuals are those who are ignorant of security policies and procedures and unintentionally create security breaches. Examples of well-intentioned violations include disabling virus protection software, using virus-laden disks or programs, or downloading shareware (Hayden, 1999).

In contrast to the above four categories, Stanton et al. (2004) identify six categories of insiders: intentional destruction, detrimental misuse, dangerous tinkering, naïve mistakes, aware assurance, and basic hygiene. The basic differences between the two sets of categories involve an added element of expertise and two additions of beneficial insiders in Stanton et al.'s categories. Intentional destruction involves persons with high expertise who have malicious intent to do harm to information systems and resources. Detrimental misuse involves those who have malicious intent, but with low expertise. These individuals engage in harassment, annoyance, and rule breaking instead of major destruction as with intentional destruction. These two categories align relatively well with traitors and zealots (Stanton et al., 2004).

Dangerous tinkering and naïve mistakes include those individuals with high and low expertise, respectively, and unintentionally weaken security measures. This includes those members who inadvertently change settings on hardware and software that provide access to outside hackers or use poorly constructed passwords. These categories are very similar to well-intentioned insiders (Stanton et al., 2004).

Finally, aware assurance and basic hygiene workers represent those high and low expertise individuals who act with beneficial intentions toward the organization. These members identify and report weaknesses in the organization's computer security and strictly follow security procedures. Organizations, obviously, desire a high number of aware assurance and basic hygiene employees (Stanton et al., 2004).

WHY INDIVIDUALS ENGAGE IN ATTACKS

Shaw et al. (1998) explain that personnel who create the information systems are the ones who are attacking them. It is also pointed out that gaining insight into the psychology of information system criminals is paramount in developing adequate protection against attacks. Hayden's (1999) research estimates that 89 percent of the attacks were initiated by disgruntled employees. Shaw et al. (1998) support this claim, citing lay-offs, transfers, and other grievances as the motivation behind the attacks. In addition to disgruntled workers, individuals seeking personal gain, well-intentioned persons, and malicious employees make up a significant portion of the remaining attacks.

Shaw et al. (1998) conducted a survey to study the psychological profile of information technology specialists who eventually undertook malicious actions after being hired by an organization. They studied full- and part-time employees; contractors, partners, consultants, and temps; and former employees who still maintained access into the information systems. For full- and part-time employees, the most common psychological theme was "greed, revenge for perceived grievances, ego gratification, resolution of personal or professional problems, to protect or advance their careers, to challenge their skill, express anger, impress others, or some combination" (Shaw et al., 1998, p. 3). For the next set of insiders, which included contractors, partners, consultants, and temps, the most prevalent cause of attack was trying to secure future work. These insiders intentionally created problems that their expertise alone could correct in the hopes that the organization would hire them. Finally, for former employees, their motivation commonly was found in the need for vengeance from their termination.

Shaw et al. (1998) also noted several key characteristics found in employees who were prone to conduct malevolent attacks. These characteristics included introversion, computer dependency, frustrations within and outside of the workplace, lack of complete loyalty to the organization, loosely applied ethical morals, and a lack of empathy. Common trends of being aggressive loners, unsuccessful in interpersonal relationships, poor team players, and anger towards authority figures were seen repeatedly in insiders. Coupling these psychological factors with a perceived hostile workplace environment increased the risk of information system specialists engaging in destructive behavior. Even with the dynamic interaction between the psychological factors and the environment, a recurring pathway was noted by researchers. This pathway included: "predisposing personal traits, an acute situational stressor, emotional fallout, biased decision-making or judgment failures, and failure of peers and supervisors to intervene effectively" (Shaw et al., 1998, p. 9). This pathway led directly to insider attacks.

Randazzo, Keeney, Kowalski, Cappelli, and Moore (2005) examined 23 insider attacks within the banking and finance sector between 1996 and 2002. Several interesting findings were annotated in their report. First, their analysis revealed that 87 percent of the attacks required very little technical sophistication or expertise. The insiders exploited business rules and policies instead of vulnerabilities of the information systems themselves. Second, 81 percent of the incidents included extensive planning by the insider and 85 percent of the incidents involved someone besides the attacker. Third, and most importantly, financial gain was the greatest motivator for the attackers. Over 81 percent of the attacks were motivated by and with the goal of financial gain. Other motivations included revenge, dissatisfaction, or a desire for respect. Some other goals, separate from motivation, included deliberate information system sabotage and stealing proprietary information (Randazzo et al., 2005).

EXAMPLES OF INSIDER ATTACKS

Examples are prevalent throughout government, public, and private organizations that illustrate successful insider attacks. The following four examples are representative of Hayden's (1999) traitor, zealot, browser, and well intentioned insider attackers. To begin, the following scenario reveals a traitor's actions in attacking an organization's information system:

> *"In March 2002, a "logic bomb" deleted 10 billion files in the computer systems of an international financial services company. The incident affected over 1300 of the company's servers throughout the Unites States. The company sustained losses of approximately $3 million, the amount required to repair damage and reconstruct deleted files. Investigations by law enforcement professionals and computer forensic professionals revealed the logic bomb had been planted by a disgruntled employee who had recently quit the company because of a dispute over the amount of his annual bonus" (Randazzo et al., 2005, p. 1).*

This second example exposes a zealot's attempt to punish an organization for its downsizing actions:

> *"A Management Information Systems (MIS) professional at a military facility learns she is going to be downsized. She decides to encrypt large parts of the organization's database and hold it hostage. She contacts the systems administrator responsible for the database and offers to decode the data for $100,000 in "severance pay" and a promise of no prosecution" (Shaw et al., 1998, p. 1).*

A third example involves a browser threat in which an insider was curious about a hacker program she developed and how it could affect the network. The employee "set up a packet spoofing application to test out her programming ability" (Stanton et al., 2004, p. 5). The final example includes a well-intentioned individual who committed an unintentional malicious act. An employee "wrote her password on a sticky note and put it on her monitor" (Stanton et al., 2004, p. 5). This provided easy access onto the organization's network and revealed a significant vulnerability.

DETECTING INSIDER ATTACKS

Detecting insider attacks on information systems have proven to be an extremely difficult task, especially since insiders have been granted authorized access to those very systems. To combat this vulnerability, Pipkin (2000) and White et al. (1996) credit intrusion detection systems as one available technique that is proving somewhat successful. Some detection systems, known as pattern-matching systems, review source and destination addresses and other network information looking for "signatures" of previous or known attack situations (Tipton & Krause, 2001; Hayden, 1999). Several intrusion detection systems, such as Network Intrusion Detection Systems, Host-based Intrusion Detection Systems, MIDAS, Network System Monitoring (NSM), and DPM, have been developed and have proven to be relatively effective (Schultz, 2002; Nguyen & Reiher, 2003). If identified in a timely manner, efforts can be made to eliminate the threat.

Pipkin (2000) references three detection methods that help in tracking and identifying network attacks, which are integral to IDS operations. First, profiles of network system operations and users are created to establish a baseline. When unusual activity is detected, it is compared against the baseline in an attempt to reveal an attack or malicious actions. Offline methods attempt to rectify known vulnerabilities before attacks can be instigated against them. The offline method commonly corrects configuration errors and other vulnerabilities through the installation of software patches. Finally, online detection methods investigate the impacts that ongoing attacks are having on the information system and its components. While an attack is in progress, efforts are taken to track down or lock the individual out of the network. By retracing the attacker's steps, security members can hopefully locate and identify the responsible party (Pipkin, 2000).

We now briefly examine three different active detection methodologies that have proven effective at detecting malicious insider activities: Fusing, Clustering, and Security Log Auditing. "Fusing" is a one method that relies on gathering "information from heterogeneous information sources" and "various levels of the IP stack…allows more accurate and timely indications and warning of malicious insiders" (Maybury 2006). Fusing combines information from multiple sources and mines the data for indicators of malicious intent. The effectiveness of the method is highly dependent upon the amount and type of observables collected as well as algorithms used to mine the data for malicious intent. Efficient detection may require the collection of a wide array of sources ranging from information sources to work environment sources as shown below in Figure 1:

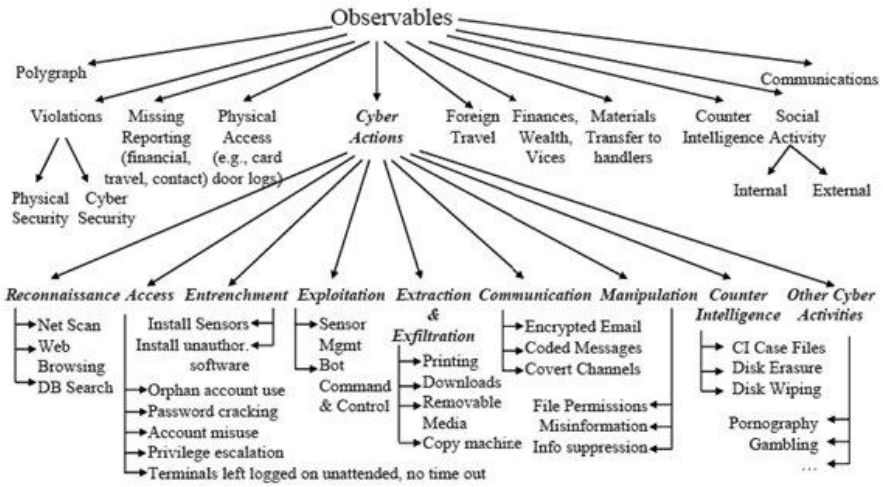

Figure 1. Observable Taxonomy (Maybury 2006)

"Clustering" is another form of method of data mining which can be used to distinguish between legitimate and malicious activity (Yang et al. 2004). Clustering attempts to categorize normal and abnormal activity by using classification techniques to group objects into subclasses that categorize the type of activity. This method relied upon the idea that if an activity does not belong to an accepted set of activity clusters, that it indicates potentially malicious activities. The method is augmented with rule-based decisions to improve its accuracy and to account for special exception situations.

Auditing of system security logs can play a critical role in insider detection (Levoy 2006). The events generated by security related activities such as directory access, audit policy changes, system logons, and system logoffs can provide valuable clues about user intent when properly collected and analyze. For example, the customization of the security policy for Windows XP can provide valuable indicators of malicious insider activities (Levoy et al. 2006). Customization can improve detection efficiency by auditing only the most informative events in order to reduce the overhead required to store and process all events. Similarly, UNIX based operating systems provide security auditing capabilities that can be utilized. Unfortunately, many organizations fail to invest the required resources or customize their auditing policies to fit their security needs (Anderson 1980).

COUNTERMEASURE DEPLOYMENT

Jajodia et al. (1998) identify prevention as the traditional method of providing information system security that minimizes successful attacks on organization's systems. Prevention is effective against individuals who do not have inside access to the systems they are attacking; however, prevention is relatively useless against insider threats. Other methods must be employed to mitigate insider attacks. Jajodia et al. (1998) recommend the following: "establishment of user privileges, appropriate system configuration, and the placement of critical system components within a security architecture" (p. 61). Additionally, strong authentication requirements, sound security policies, implementation of the "need-to-know" principle, and security awareness education and training also play vital roles in countering insider threats.

Although commonly overlooked, psychological considerations, as mentioned above, play a significant role in insider attacks, and by recognizing them, organizations can effectively secure their systems. Managers need to address the psychological aspect of the insider threat. Shaw et al. (1998) recommend effective intervention by family members, fellow employees, and managers, including counseling, support groups, or medical expertise as applicable. This intervention action has shown to diffuse the risk of insider attacks. Theoharidou et al. (2005) acknowledge the General Deterrence Theory as the classical criminology theory behind deterring crime and is effective against insider threats. When the possibility of punishment exists and is well know and the penalty is of a severe nature, potential attackers will be dissuaded from engaging in attacks. Thus, by combining strong internal security policies and procedures with psychological considerations, organizations can counter, and hopefully mitigate, potential insider attacks.

CONCLUSION

To successfully operate in the Information Age, organizations that rely on information systems must provide robust, layered, network security by understanding all facets of insider threats: what they are, the negative impacts they create, which employees are most likely to commit an attack and why, detection of the attacks, and defending against them. Computer crime is continually increasing, along with organizational reliance on information systems. If businesses desire to continue to operate, they must understand the vulnerabilities and risks associated with insider threats and implement sound security practices to defend against them.

DISCLAIMER

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the U.S. Government.

REFERENCES

1. Anderson, J. P. (1980). Computer Security Threat Monitoring and Surveillance, Fort Washington, PA Contract 79F296400, April 15, 1980. http://csrc.nist.gov/publications/history/ande80.pdf
2. Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2006). 2006 CSI/FBI Computer Crime and Security Survey. Washington, D. C.: Computer Security Institute Publications.
3. Hayden, M. (1999). The Insider Threat to U.S. Government Information Systems. Maryland: National Security Telecommunications and Information Systems Security Committee.
4. Jajodia, S., Ammann, P., & McCollum, C. D., (1999). Surviving Information Warfare Attacks. Computer, 32(4), 57-63.
5. Levoy, T. E. (2006) Development of a Methodology for Customizing Insider Threat Auditing on Microsoft Windows XP Operating System, Master of Science Thesis: Air Force Institute of Technology, 2006.
6. Levoy, T. E., Grimaila, M. R., & Mills, R. F. (2006). A Methodology for Customizing Security Auditing Templates for Malicious Insider Detection, Proceedings of the 8th International Symposium on System and Information Security (ISSIS 2006); Sao Jose dos Campos, Sao Paulo, Brazil; Nov. 08-10, 2006.
7. Maybury, M. Detecting Malicious Insiders in Military Networks, in MILCOM-06 Washington, D.C., 2006.
8. Nguyen, N. & Reiber, P. (2003). Detecting Insider Threats by Monitoring System Call Activity. Submitted to 4th Annual IEEE Information Assurance, West Point, New York.
9. Pipkin, D. L. (2000). Information Security Protecting the Global Enterprise. New Jersey: Prentice Hall PTR.
10. Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A., (2005). Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector. U.S. Secret Service and CERT Coordination Center: Software Engineering Institute.
11. Schultz, E. E. (2002). A Framework for Understanding and Predicting Insider Attacks. Computers and Security, 21(6), 526-531.
12. Shaw, E., Ruby, K. G., & Post, J. M., (1998). The Insider Threat to Information Systems The Psychology of the Dangerous Insider. Security Awareness Bulletin, 2-98, 27-46.
13. Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2004). Analysis of End User Security Behaviors. Computers & Security, 1-10.
14. Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The Insider
15. Threat to Information Systems and the Effectiveness of ISO17799. Computers & Security, 24, 472-484.
16. Tipton, H. F. & Krause, M. (2001). Information Security Management Handbook, 4th Edition, Volume 2. New York: Auerbach.
17. White, G. B., Fisch, E. A., & Pooch, U. W. (1996). Computer System and Network Security. New York: CRC Press.
18. Yang, D., Hu, C., & Chen, Y. (2004). A Framework of Cooperating Intrusion Detection based on Clustering Analysis and Expert System. In Proceedings of the 3rd international Conference on information Security, 85, 150-154.