The Persistent Insider Threat

Is Enough Being Done?

In today's world, the main asset for businesses is the data they store. As enterprises become more dependent on technology and data, it becomes increasingly important to protect the data and ensure the security of the systems. Broadly speaking, there are two threats that put data and organizations at risk: insider threat and outsider threat.

Insider threat has been discussed on and off for years, but it seems that whenever there is a breach that is caused by an insider, there are discussions on how this threat is mitigated. Eventually, these discussions wane and seem to be of only occasional concern. On the other side of the coin, there is constant discussion on keeping boundaries safe and keeping the bad guys out. So why does the momentum for insider threat seem to lose traction? Insider threat may be as great as outsider threat because it is so hard to mitigate. How does an organization keep control of the very people to whom it must give access?

Defining Insider Threat

Insider threat can be defined as the danger posed when the data and systems belonging to the organization are put at risk by trusted personnel.[1] This threat can come from anyone within the organization. Outsider threat is always an intentional act by someone to gain access to a system. However, insider threat may be an intentional or unintentional act. Personnel may unintentionally expose sensitive data to the outside world without even knowing it. In trying to perform their job, they may put a hole in the security of the network without realizing it. These threats are harder to control because the personnel who must have access to the systems and data to complete their job requirements are the same personnel who must be controlled on the network. This access automatically creates a vulnerability that may be exploited. Whether the threat is intentional or not, it is still very real and must be dealt with in any organization.

A Look at Insider Attacks

To better understand insider threat, it is beneficial to look at attacks that have already occurred. There were five attacks that occurred in 2012 that show different ways systems can be exploited:[2]

- Barnes & Noble announced that 63 of its stores had nefarious personal identification number (PIN) pads installed that allowed someone to pull the credit and debit card numbers as well as the PINs to customers' bank accounts. Although this was an insider attack, the resulting investigation did not reveal how the attack occurred.
- Many boardrooms and meeting rooms across the world have videoconferencing systems installed. Many companies want the best technology, but do not always understand the security risk that new technologies bring into the organization. Research by Rapid7 has shown that many video and teleconferencing systems can be accessed directly from the Internet. In a scan of only a small percentage of the Internet's address space, Rapid7 discovered that around 5,000 of these systems were set up to automatically answer Internet calls. This access could potentially be used to listen to conversations and, in some cases, read information on whiteboards.

Rodney Piercy, CISSP, CEH
Is an information technology security manager for the US Army. After retirement from active duty in the US Army, he served as a senior systems analyst, network defense manager, chief network security officer, security architect, chief technology officer and chief information officer for organizations within the US Army. He has experience in various domains of information security including certification and accreditation, vulnerability assessment, incident response, mobile security, and network security. He led a team in research on mobile security that developed a mobile application testing capability currently used by the US Defense Information Systems Agency. He has also participated as a speaker on mobile security at the Cybersecurity Summit.

- In California, USA, an employee left a company and took 760 files with him to his new company. This created a lawsuit between the two companies over intellectual property. This type of information must be controlled tightly to prevent theft.
- In South Carolina, USA, an attacker gained insider access by getting an employee's credentials. This access allowed the attacker to obtain 3.6 million Social Security numbers and 387,000 credit and debit card numbers. The cost for this attack was estimated to be at least US $14 million. This type of attack is usually due to carelessness on the part of the employee and is not a malicious act of the insider. Employees must be trained on how to keep their credentials safe.
- The Swiss intelligence agency reported that a system administrator was able to take terabytes of classified data out of an organization on hard drives, but investigators are not sure what the employee did with the data. In many organizations, system administrators are not restricted and can access any information on the system.

Motivation Behind Insider Threats

To understand any threat, there must be an understanding of why the threat exists. Since the threat can be either unintentional or intentional, both areas must be considered. The unintentional threat normally comes down to personnel rushing through their tasks, displaying a careless attitude, or not having appropriate training or experience. These risk factors are easily mitigated.

The more difficult risk to mitigate is the intentional insider threat. There may be many different reasons for the attacks.[3] Some will join an organization with the intent to do harm and others become disgruntled over time or become desperate due to their situations. Motivators include politics, power, fear, greed, revenge, excitement or general malice. Since these are powerful motivators, organizations need to understand how and when these motivators are affecting their employees.

The goal of any security program is to stop the threat before it becomes an incident. The insider threat is no different. Personality traits can play a significant role in finding and stopping the insider threat. Some studies have looked at personality traits and how they relate to psychosocial factors. The most prevalent traits were low conscientiousness, low agreeableness and neuroticism. According to the study, the way people write tells a lot about their personality. Since employees communicate through electronic means, their daily writing can be monitored and captured. Word studies have been done that can relate the words that are used and how they are used to specific psychosocial factors showing the concerning personality traits. This type of monitoring can show which employees show tendencies toward being an insider threat.[4] If an organization is using this type of technology, it must be careful not to cross the line into privacy and ethical issues.

> **"Social engineering is an area that could be considered both an insider and an outsider threat."**

Social engineering is an area that could be considered both an insider and an outsider threat. Social engineering starts as an outsider threat, but is dependent on the insider doing something. The insider may not have any intention of hurting the company, but may do so if he/she falls prey to a social engineering attack. Since this type of attack requires the insider to do something, the insider also has the power to stop this kind of attack.

Organizations have a good understanding of outsider threats and how to mitigate them, making

Enjoying this article?

- **Learn more about, discuss and collaborate on cyber security in the Knowledge Center.** *www.isaca.org/cybersecurity-topic*

it more difficult for attackers to break in from the outside. An attacker will normally take the path of least resistance to the target. This makes an insider an easier target for outside attackers if the inside path is not as well guarded as the outside. Other factors make employees more susceptible to being used and/or becoming complicit in an insider attack. As an example, the economy may have an effect. When the economy falters, people get into financial trouble and become desperate. This creates a vulnerability for an external source to exploit.

Cost of Insider Threats

To know if the risk is worth mitigating, an organization must understand not only the cost of the mitigation, but also the cost of the incident, should it occur. There are several costs that must be counted when completing this calculation:

- The worth of the lost data
- The damage to equipment
- The loss of money
- The cost of cleanup
- The cost of fixing the vulnerability that was exploited
- The loss of revenue from downtime
- The loss of revenue due to the loss of customer trust and company image
- Legal fees and court costs
- In some cases, considerations related to restitution to customers, injury, death and national security

Although this list may not be exhaustive, it is a good indicator of the many factors and costs involved with an insider threat. So with all of these factors, how much might an incident cost? A survey constructed by the SANS Institute found that most respondents did not know what the actual cost of a breach caused by an insider might be, but 19 percent said the potential loss could be US $5 million dollars per incident.[5] Each organization will be different depending on the type and importance of the information it stores, but the results of an incident caused by an insider will be costly for any organization.

"In the relationship between security budget and cost of attacks, things seem to be a little backward."

The Ponemon Institute's *2015 Cost of Cyber Crime Study* contains some interesting findings. Attacks by malicious insiders were the most costly type of attacks and took longer to resolve than other attacks. In the relationship between security budget and cost of attacks, things seem to be a little backward. Even though malicious insiders are the most costly and cause the longest downtimes, only 13 percent of the security budget is being spent on the human layer.[6]

Mitigation

Although there are many variables to insider threats, this is an area that should not be taken lightly. Every organization mitigates the risk of insider threats a little differently, but it can be broken down into just a few categories, including:

- Hiring practices
- Policies and procedures
- Training
- Culture
- Automation

The methods each organization uses are largely dependent on the organization itself, depending on the type and amount of data the organization is trying to protect, the importance of the data, the knowledge of the personnel implementing the mitigation, the available budget, and leadership buy-in.

Mitigation Strategies

When looking at outsider threats, most security professionals look at a structure called defense in depth. This structure consists of several layers of security of varying types that someone would have to work through to be able to damage the organization. However, the better the security capability, the harder it is to get in from the outside, which makes using an insider an easier method of attack. Since the defense-in-depth method has been effective in addressing outsider threats, security professionals should use it when considering insider threats, but with caution. Since insider threats deal directly with employees, any mitigation used must be within the privacy rights of the employees.

Since there are two types of insiders, there must be two types of strategies. The first set of strategies are those that are directed at the employees who are not intending to do harm:

- Organizations must put in place policies and procedures—most already have these. They should be very specific as to what is expected from the employee and the many different types of attacks they may encounter. The user should be able to identify these attacks and understand what response the organization wants them to have. The policies should be reviewed periodically to ensure that they still meet the objectives for which they were designed. There should also be some form of consequences if policies and procedures are not followed. If there are no consequences, there is no motivation to follow procedure.
- An organization cannot rely on policies and procedures alone. There must be some type of automated controls. One such control should be a separation of duties for system administrators. A system administrator should not have complete and unsupervised access to all of the organization's information. Dividing the system administrator duties among different personnel and allowing them only the access they need for those duties reduces the risk.

"An organization cannot rely on policies and procedures alone. There must be some type of automated controls."

- Training is another area that must be considered when looking at insider threats. Employees must know how they should react to threats. Training must be interesting and relevant to be effective. Training that cannot be related to the everyday work environment will not be taken seriously by the employees and will be ineffective. Supervisors should have additional training in recognizing the personality traits and attitudes that may be a precursor to an insider attack.
- An area that is not taken into consideration by many organizations is culture. The culture of the organization can play an important role in mitigating insider threats. If employees feel they are important and valued by the company, they are more loyal to the organization and less likely to do something that is damaging. They are also more likely to report someone else who is doing something that could be damaging to the organization. If the organization has a good culture and takes care of its employees, not only

is the insider threat reduced, but longevity and motivation may be increased as an additional benefit.

- Along with having a good work environment and culture, organizations must understand and know their employees. This does not happen just when they are hired; it must be an ongoing process. Immediate supervisors play an important role in this area. There are many outside factors that can affect and influence employees. Outside influences can affect employees through social engineering or other means, and the organization must know what these factors are and the effect they have on employees. Supervisors who have a good relationship with employees may be more likely to know when something changes in the life of an employee. Such changes may develop or expose areas of weakness that could be exploited by outside factors. Supervisors who are aware of the changes when they happen may be able to take action prior to a threat becoming realized.

The reality is that although mitigations for the average employee are needed, they will be limited in their effectiveness because only those employees who are trying to do the right thing will adhere to them. If someone intends to harm the organization, these mitigations will have little to no effect. There should also be strategies in place to mitigate the insider who intends to do harm:

- Human resources (HR) has the first opportunity to stop an insider threat. Some organizations use social media to vet new employees. During the hiring process, the organization has the opportunity to learn as much about prospective employees as possible. HR must try to learn their likes and dislikes, their biases, and any areas of weakness that could be exploited by an outsider.
- There are ways that automation can help. Although building automated policies can be time consuming, a digital management system can automate policy management in real time.[7] Any violations to these policies can then be sent to the intrusion detection system (IDS) so that security personnel may be notified and the incident logged. This kind of early warning can reduce the damage caused by an attack.
- Many times, the individual's actions are difficult to track through automated means, but an insider attack can take a toll on the network and the network can give clues to what is going on. Organizations can then monitor for and track these clues to find and stop an insider attack. Some of the clues are irregular memory usage, irregular web site usage, file system or memory manipulation, resource overutilization, and the use of unauthorized protocols.[8] Some of these could be network issues, but they may also be attacks that have not been recognized.

Conclusion

Insider threats are one of the most difficult threats to deal with because the very users who must have access to the networks and data are also the users who may cause damage to those same networks and data. It is difficult to review statistics for insider attacks because many organizations handle them internally and do not report them to the authorities. Sometimes organizations do not even know they have occurred or may not want to risk the company being embarrassed. Statistics make it easier to learn from the mistakes of others, but if attacks are not reported, others cannot learn from them and, therefore, they may make the same mistakes.

"It is difficult to review statistics for insider attacks because many organizations handle them internally and do not report them to the authorities."

When planning for outside threats, security professionals use a good defense-in-depth security plan to protect the network. The same defense-in-depth concept should be used when planning protection against inside threats. Security professionals must take a holistic approach when building security plans to ensure that they include multiple layers of security for both insider and outsider threats. All of the areas discussed in this article can be used as a layer of defense that can be

applied within an organization. Some of the areas are easier and less costly to implement than others, but if multiple layers are used, the risk of insider threat can be greatly reduced. Organizations must be as vigilant with insider threats as they are with outsider threats.

Endnotes

1 Maasberg, M.; N. L. Beebe; "The Enemy Within the Insider: Detecting the Insider Threat Through Addiction Theory," *Journal of Information Privacy and Security*, vol. 10, iss. 2, 16 July 2014, p. 59-70

2 Dark Reading News, "Five Significant Insider Attacks of 2012," *InformationWeek*, 17 December 2012, *www.darkreading.com/vulnerabilities---threats/five-significant-insider-attacks-of-2012/d/d-id/1138865*

3 Contos, B.: D. Kleiman; *Enemy at the Water Cooler: Real-life Stories of Insider Threats and Enterprise Security Management Countermeasures*, Syngress, USA, 2006

4 Greitzer, F. L.; L. J. Kangas; C. F. Noonan; C. R. Brown; T. Ferryman. "Psychosocial Modeling of Insider Threat Risk Based on Behavioral and Word Use Analysis," *e-Service Journal*, vol. 9, iss. 1, October 2013, p. 106-138

5 Cole, E.; *Insider Threats and the Need for Fast and Directed Response*, SANS Institute, April 2015, *www.veriato.com/docs/default-source/whitepapers/insider-threats-fast-and-directed-response.pdf?sfvrsn=14*

6 Lord, N.; "Findings From the 2015 Ponemon Institute Cost of Cybercrime Study: The Threats vs. Defenses Gap," *Digital Guardian*, 18 November 2015, *https://digitalguardian.com/blog/findings-2015-ponemon-institute-cost-cybercrime-study-threats-vs-defenses-gap*

7 Barrios, R. M.; "A Multi-leveled Approach to Intrusion Detection and the Insider Threat," *Journal of Information Security*, vol. 4, iss. 1, January 2013, p. 54-65

8 Magklaras, G. B.; S. M. Furnell; P. J. Brooke; "Towards an Insider Threat Prediction Specification Language," *Information Management & Computer Security*, vol. 14, iss. 4, 2006, p. 361