Global Information Assurance Certification Paper

Internal Threat – Risks and Countermeasures

Jarvis Robinson

November 15, 2001

Version 1.0

Background

Many of us were told the story of Benedict Arnold. If you are unfamiliar, Benedict Arnold was the U.S. Army officer during the Revolutionary War who turned traitor. Benedict conducted secret propositions with the British that could have cost the U.S. the war and changed history. Fortunately, Benedict's plot was uncovered and the British were defeated. This type of threat has not changed much since the days of Benedict Arnold. Not only does it continue today, but technology has also made it more prevalent.

Considering the recent media attention given Internet-based attack, it is no wonder why many organizations are so focused on firewall and web server security. As a result, many organizations fail to realize the looming threat of attack from the inside. This document will show that such failure can be quite costly. Additionally, this document will cover the risks associated with insider threat. Last, this document will provide practical counter-measures, which should challenge the reader to focus on the people and processes that protect information rather than technology.

Examples

According to the 1999 Computer Security Institute/FBI report, 55% of respondents reported malicious activity by insiders. Although it seems like science fiction, insider threat has been prevalent throughout the course of information technology. As an example, Information Security Magazine references the American Society for Industrial Security (ASIS) survey of Fortune 1000 companies in 1997. Based on the survey ASIS determined that companies in the U.S. "could be losing over $250 billion annually" to espionage. The survey identified over 1,000 incidents of theft, which were worth an estimated $44 billion. Considering the losses in the 1997 survey was reported as "five times greater" than the previous survey, it seems to indicate that matters have not improved.

Depending on the goal of the attacker, damages could range from malicious tampering to loss and unauthorized distribution of proprietary assets. If insider attacks still seem unlikely, consider that insiders make the most qualified culprits when it comes to information compromise. After all, insiders have the means to access the information we protect so vigilantly from attackers on the outside. Along this line of thought, we must challenge ourselves to not only secure information in transit (i.e. HTTPS/SSL) but also secure destination points, which are accessible to insiders (i.e. database security).

Information Security magazine references an assessment from the Computer Security Institute (CSI), which stated, “the average insider attack cost the target enterprise $2.7 million, compared with $57,000 for the average outside attack.” To illustrate the costliness, the FBI states that the National Library of Medicine (NLM) computer system was compromised in January and February 1999. The FBI mentioned that through the intrusion, system administrator passwords and several hundred sensitive files were downloaded. Considering the NLM provides thousands of medical professionals with breaking information on topics such as diseases, treatments, and dosage units the intrusion was viewed as a severe threat. Through FBI investigation, the intruder was identified as a former computer programmer for NLM, who managed to create a “backdoor” while he was employed there. Although the programmer was arrested and convicted the damage was already done. This intrusion resulted in loss in excess of $25,000.

It could be said that insider attacks represent the most prevalent of all threat. Instead of reliance in technology, business operation and information protection is at the mercy of human compliance. In essence, we must trust that humans make the right decisions and follow the processes or policy needed to protect information. For example, defending against social engineering requires a high degree of compliance with security policy and processes. As such, technology can do little to counteract it.

Social engineering is the process of exploiting humanistic weaknesses such as the desire to help those in need. The attacker’s objective is to gain the information needed to carry out an attack or escalate privilege. For example, an insider could call a friend working in the support center in order to gain unauthorized privilege to server. Or an insider could claim that a request is for the senior manager of the enterprise in order to pressure the help center resource into subverting security policy. In many cases, a sense of urgency or consequence is enough to breakdown conventional processes. Unfortunately, support resources are challenged with making these types of moral decisions every day. Therefore, it is important to realize that people are a more critical element of security than technology.

Motives

So why do insiders risk their livelihood in order to attack the organizations that employ them? In many cases, inside attacks are attributed to behavioral conditions. Along this path, disgruntled attackers represent a severe threat. Given the technology afforded the disgruntled employee, he or she may feel more gratification through destroying data rather than displaying discontent at the employee picnic. In many cases, disgruntled employees are simply dissatisfied with their place of employment while in other cases the network just seems like a good place to vent anger.

Other insiders attack not for vengeance but for the sake of testing their skills or causing mischief. While they seem harmless, such attackers should be treated as seriously as any other threat to information assurance. Last, attackers with a

financial motive may use their access to steal proprietary information and even sell trade secrets to competitors. Although it's every security professional's nightmare, corporate espionage does occur.

Practices

Although insider threat seems almost impossible to contain, measures do exist to help mitigate the risk therein. At a minimum, organizations should be vigilant with background checks on candidates for hire. This tactic may uncover any criminal background, which the candidate was not forthright with. To take it a step further, organizations should understand the characteristics of at-risk employees and screen accordingly. Behavioral surveys are one option that could serve as a good supplement to an interview.

In some cases, access to resources is granted to insiders on demand and often without justification. Unfortunately, failure to validate access could easily result in unauthorized access or "backdoors" as described earlier with the National Library of Medicine example. While it does require time and resources, consistent re-verification practices could reduce the chance of an inside attack and the costs therein. In its simplest form, re-verification may consist of periodically validating resources such as sensitive user accounts, group membership, and access control lists. A loftier goal could entail a re-verification of all sensitive and "non-sensitive" resources.

Typically, system administrators represent carte blanche' access to systems throughout the organization. As such, they should be the principle focus around re-verification practices. Specifically, organizations must obligate themselves to re-verifying users who posses administrative rights. Additionally, user groups must be re-verified to ensure that group members are warranted.

For a security to be effective, re-verification should be a standard practice that is carried out frequently. Depending on what is acceptable risk, the list of resources may include user accounts, group membership, data access control lists, and the owners therein. Due to factors such as time and cost however, an organization may be reluctant to carry out a full-scale re-verification of their resources. In such cases, the re-verification interval could be staggered according to the sensitivity of the resource.

To illustrate, the Enterprise Admins group was created with the advent of Windows 2000. This group shuns the privileges afforded the Domain Admins group in the sense that members of the Enterprise Admins have full access to any domain that is joined to the enterprise structure named a forest. In this case, it would befit security to re-verify the Enterprise Admins group membership on a more frequent basis than less sensitive groups. It is important to note that the success of the process depends on user compliance from start to finish. If security administrators or the owners they notify are untimely with their responsibilities, then re-verification could become ineffectual.

Physical security must also play a role towards protection within the perimeter. Such measures include storing servers and other critical nodes in a locked room only accessible by authorized resources. For more sensitive servers such as firewalls, consider locking them in a cabinet or cage so as to restrict the ability to power off or access the local drives. Similar to network security, the list of individuals who are authorized to access the servers should be re-verified as much as possible. On a similar note, any physical access afforded an employee or contractor should always be revoked or denied upon termination. This would include revocation of ID badges and changing key codes on doors that lead to sensitive entrances or exits.

Security is always as strong as its weakest link. As such, end-users must play a role in protecting information too. Users should demonstrate physical security should by always locking their portable devices (i.e. laptops). Most docking stations provide the ability to lock the laptop onto them. In cases where dock locking is inadequate, a strong locking cable could be attached to the laptop or dock. While this does not eliminate the exposure to an attacker, it creates additional time required to steal the portable device. Given a choice, an attacker would probably pursue a less conspicuous target.

For many organizations, critical information is within an attackers grasp or walking distance. Technical diagrams containing sensitive specifications are 'low hanging fruit' for passersby. For example, diagrams could contain information such as TCP/IP addresses and configuration settings such as ports and access control lists. Therefore, technical diagrams should never be made accessible to unauthorized users. Such careless leaves much to the imagination including the threat of theft. While simplistic, safeguards such as storing removable media and confidential documents in a locked bin are sometimes overlooked.

When complied with, policy plays an effective role in reducing insider threat. For example, a usage policy is a contemporary document that clearly stipulates acceptable usage for information systems. It should convey, to users, the penalties they could be subject to if they violate the policy. In essence, the policy should leave little room for assumption. Additionally, a security policy is essential. This is similar to a usage policy but is targeted towards the organization's overall vision and philosophy towards a "secure" environment. This could include broad topics such as organization's position on user administration (i.e. password and ID guidelines) and physical security requirements.

In order to fully assess the level of cooperation the policy has received, compliance activity is necessary. Specifically, compliance involves auditing systems and users to ensure that the controls set forth in the policy are enforced. Essentially, compliance activity allows organizations to determine their strengths and weaknesses. Similar to re-verification, timeliness is critical to the success of compliance. After all, systems that are out of compliance represent a weakness in the 'chain of defense'. As a result, weak systems and

users who fail to follow policy provide an avenue of attack.

Security awareness is the process of educating end users on the threats and risk to confidentiality, integrity, and availability. Security awareness is a proactive method towards education that could aid in the prevention of an attack. As such it can be a powerful countermeasure to insider attacks. Dissemination methods may include periodic security newsletters, security fairs, and conventional training.

To say the least, a mere security awareness newsletter distributed via e-mail may be an inexpensive method that could help users protect themselves from attack. Potential messages could outline social engineering, the importance of compliance, and physical security. Ultimately, the cost of an attack could easily overshadow the cost of establishing a security awareness program. Therefore, organizations should spend the effort upfront instead of adding to the risk factor.

When all else fails, there must be a resource or team that is prepared to detect, respond, and recover from attacks on the network. An incident response team satisfies this need. Considering the growing number of security events, this team is necessary if the operation of business is critical. Organizations such as SANS and the Carnegie Mellon's CERT provide this type of service but on a broad scale. For example, SANS and CERT typically provide timely reports on newfound vulnerabilities as in the case of the Code Red worm and Nimda virus.

Since organizations such as SANS and CERT provide incident response on a broad scale, incident response is still required internally to meet the needs of the enterprise. Conventionally, an incident response methodology should be indoctrinated in processes involving the team as well as processes within other IT teams in the organization. For example, the network monitoring team responsible for infrastructure should have a clear understanding of steps and conditions involved with engaging the incident response team. Any room for assumption could result in loss of operations and revenue.

Summary

The story of Benedict Arnold is proof that insider threat is real. In Benedict's case, his treacherous plot was uncovered in time for America to realize his intentions. However, many organizations today will not be so fortunate with counteracting inside attacks. As mentioned earlier, the losses associated with insider attacks can be more damaging than those caused by outside attacks. However, insider attacks share a common thread with those from the outside; regardless of the threat origin, the damages could include loss of revenue and a tarnished company brand.

This paper has provided an illustration of the issues relative to insider threat and recommended countermeasures. While insider threat may never be eliminated, it is worth noting that risk-mitigating countermeasures do exist. Such measures include re-verification, security awareness, security policy, compliance activity,

and physical security. When countermeasures become futile, it is important to have an incident handling process in place.

For those who value confidentiality, integrity, and availability, it is important that security efforts be focused around all aspects of the enterprise. Specifically, each organization's security architecture must take insider threat into account. As reiterated throughout the security industry, defense in depth is the essential. Defense in depth requires security professionals to take a layered approach to protecting information. In essence, we should never rely on just one security method or technology. Also, a defense in depth strategy should always recognize that the threat is multi-faceted. Remember that each weakness is yet another avenue of attack. As such, always consider insider threat.

List of References

DENNING, DOROTHY E. "INDUSTRIAL ESPIONAGE
Who's Stealing Your Information?" Information Security Magazine. April 1999. URL:
http://www.infosecuritymag.com/articles/1999/aprilcover.shtml

POST, JERROLD, SHAW, ERIC, and RUBY, KEVEN. "MANAGING THE THREAT FROM WITHIN." Information Security Magazine. July 2000. URL:
http://www.infosecuritymag.com/articles/july00/features2.shtml

"Establish a policy and procedures that prepare your organization to detect signs of intrusion." Carnegie Mellon University. 2000. URL:
http://www.cert.org/security-improvement/practices/p090.html

Berst, Jesse. "The Biggest Threat to Your Network's Security. (It Isn't What You Think)." ZDNet Anchor Desk. April 1998. URL:
http://www.zdnet.com/anchordesk/story/story_1959.html

The Insider Threat: Examining the Loss and Protection of an Organization's Proprietary Information. Linthicum: Silent Runner, 2000.

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor