"Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XX – 2017 – Issue 1
The journal is indexed in: PROQUEST / DOAJ / Crossref / EBSCOhost / INDEX COPERNICUS / DRJI / OAJI / JOURNAL INDEX / I2OR / SCIENCE LIBRARY INDEX / Google Scholar / Academic Keys/ ROAD Open Access / Academic Resources / Scientific Indexing Services / SCIPIO / JIFACTOR

INSIDER THREAT DETECTION AND MITIGATION TECHNIQUES

Vlad-Mihai COTENESCU[1]
Sergiu EFTIMIE[2]
[1]Military Technical Academy - Electronic Ph.D. Student Eng., Information and Communication Systems for Defense and Security Doctoral School, vlad.cotenescu@gmail.com
[2]Military Technical Academy - Electronic, Inf. Ph.D. Student Information and Communication Systems for Defense and Security Doctoral School, sergiu.eftimie@gmail.com

Abstract: *Most of the organizations these days are focusing on building their security program in order to stop malicious outsiders from affecting the confidentiality, integrity and availability of data. Inthis process, organizations are investing large sums of money and a lot of man hours. Although security controls like antivirus, proxies, firewalls, etc. are efficient to stop most of the attacks carried out by external perpetrators, they can be rendered useless when an attack is carried out by a trusted internal resource. The threat that insiders pose to businesses, institutions and governmental organizations continues to be of great concern. Recent industry surveys and academic literature provide great evidence thatshows the significance and the impact that this threat can pose.*

This paper will discuss the main factors that can help an organization to improve its security to protect against internal attacks.

Introduction

The increasing number of incidents related to insider threats attracted an elevated interest from the public, government, research and commercial sectors. Disgruntled employees or individuals that are looking to make a fast profit can use various methods in order to disrupt or cease normal business operations. Insiders have trusted status that can provide malicious parties opportunity for advanced mischief.

If that wasn't enough, bad things are happening much faster. Not only are our businesses always on, the attackers don'ttake breaks, ever. New exploits are discovered, 'weaponized', and distributed to the world within hours. So we need tobe constantly vigilant and we don't have much time to figure out what's under attack and how to protect ourselves beforethe damage is done. Compound these 24/7 demands with the addition of new devices implemented to deal with newthreats. Every device, service, and application streams zillions of log files, events, and alerts.

Hypothesis:

The real issue is pretty straightforward: of all the things flashing at us every minute, we don't know what is really important. We have too much data, but not enough information. This plentitude of data needs to be normalized and correlated in order to become meaningful and actionable.

Discussion:

An insider threat can be considered a malicious insider that is a current or former employee, business partner or contractor and meets the following criteria:

- Has or had authorized access to on organization's network, system or data
- Has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems

According to the US CERT Insider Threat Center the following aspects are observed occurring in conjunction with the usual threat posed by a current of former employee:

- Collusion with outsiders
- Insider crimes perpetrated by employees of trusted business partners
- Risks inherited through a merger or acquisition. Through a merger the risk of compromise increases if a thorough sanitization check is performed before the integration is performed.
- Internal or external political factors that might influence individuals to take action against an organization [5].

The threat of attack from insiders is real and substantial. The *2011 CyberSecurity Watch Survey*, conducted by the U.S. Secret Service, the CERT Insider Threat Center, *CSO Magazine*, and Deloitte, found that in cases where respondents could identify the perpetrator of an electronic crime, 21% were committed by insiders [SEI 2011]. In addition, 43% of respondents had experienced at least one malicious, deliberate insider incident in the previous year. The survey also revealed that 46% of the respondents thought that damage caused by insider attacks was more severe than damage from outsider attacks [3]. According to the survey, the most common insider e-crimes were

DOI: 10.21279/1454-864X-17-I1-060

- unauthorized access to or use of corporate information
- unintentional exposure of private or sensitive data
- viruses, worms, or other malicious code
- theft of intellectual property (IP)

Looking at the cyber investigations undertook by the FBI shows that the financial loss resulted from the attacks of disgruntled former employees can range from $5000 to $3 million.

In some of the mostfamous cases we can see that only one employee can cause significant damage or loss. In February 2014 Barclays Bank lost control to 27000 customer files that worth millions on the black market.

In the same period Target reported that one of its contractors was responsible of the biggest data breach in history. Target reported losing 40 million customer credit card data and 70 million customer entries containing addresses, phone numbers and names.

In March, DuPont announced that its proprietary formula to cleanly manufacture the white pigment used in paper and plastics was stolen and sold to a competitive Chinese company in the $14 billion market. A contractor working for DuPont sold the formula for $28 million in contracts. The contractor was found guilty of 22 counts of economic espionage, trade-secret theft, witness tampering and making false statements.

As we can see, from these examples, the most damaging way an insider can compromise an organization is to steal its intellectual property (AP).

Insiders can be stopped, but it is not an easy task. Insider attacks can be prevented through a layered defense strategy consisting of policies, procedures, and technical controls. The security team in conjunction with management need to pay close attention to many aspects of the organization. These aspects can include its business policies and procedures, technical environment or the culture of the organization.

Although all these aspects are important it is near to impossible to protect 100% of the assets from all internal or external threats. Having this in mind an organization needs to have a risk based exercise to identify their critical data and assets. Based on this exercise they need to put controls in place that can prevent their compromise from internal and external threat agents.

The organization needs to study its threat landscape in order to assess enterprise risk. Some of the attacks carried out by insiders are:

- Finding workarounds in order to circumvent controls that limit usage of a system.
- Trying to have a system perform something that isn't intended for
- Making an unintentional mistake
- Trying to identify vulnerabilities or weaknesses in order to report them.
- Carrying out harmful activities from various reasons like greed, delusion, fame or loyalty to another party [6].

Besides knowing the assets that need to be protected and the attacks that can be carried out it is very important to know who is being authorized to use the company systems. Usually this activity takes place at the profiling phase by meeting those individuals in person. After this step they will be associated with a role that has certain permissions associated.

Employees need to be authorized only to those systems and areas that are essential to carry out his/her duties. Granting access based on roles limits exposure and strengthens accountability [1].

Another protection that can be put in place is to assign information owners or custodians. These owners are usually people with high positions in the organization. They will own the data and based on the importance that it has they will make decisions on who is supposed to get access to it. Under the guidance of the owner, the custodian must ensure the security (confidentiality, integrity, and availability) of the asset is maintained.

Access rights need to be evaluated periodically. A big problem that organizations face is the one related to legacy permissions. Usually, companies start from a small number of employees. At the beginning, these employees perform multiple tasks and hence they hold multiple access rights. As the company grows these employees start delegating some of their responsibilities to others. Their access rights need to be adjusted along site with their responsibility changes.

The problem there is that organizations focus their effort on giving access to employees and do not focus enough time in removing access when they move to different roles. For example, if an employee starts as a network engineer, after three years becomes a manager and after another three he gets promoted to director of operations it probably means that his access requirements are significantly different than when he started.

Another big risk to organizations is introduced by storage media or access to other cloud storage solutions. Using legitimate sharing platforms or communication channels employees can easily

DOI: 10.21279/1454-864X-17-I1-060

perform exfiltration of data. Along with relying on networks to send and receive data, employees can also take advantage of local data portability from their desktop or laptop via CD/DVD burners or even USB thumb drives. Once the data leaves the company it's near to impossible to ensure its security.

In order to improve the awareness of the security team on how data is being used or accessed throughout the network organizations need to implement solid logging and monitoring applications. Along with this, all changes to production data and systems should also be logged to include what change was made, when it took place, and by who.

Logging and Monitoring should be also tweaked in order to focus only on those assets and data that was identified as being critical to the organization [2]. Gathering logging data on all the assets would be impossible to achieve. After this solution is in pace it's of the upmost importance to make sure the entries can't be modified or deleted. If system administrator can delete or manipulate their own log entries, then it is impossible to prove their integrity.

It's not enough to collect logging data. This information needs to be actionable and needs to provide meaningful alerting. The amount of log data that is being collected might become overwhelming that is why it is essential to have in place good filters and alerting rules. These rules should be tuned by experienced individuals in order to reduce the noise and the false positive count to a minimum.

Conclusion

In conclusion, every organization faces the risk of an insider attack. This risk can be adequately reduced with proper measures and preparation. The information security program should find the perfect balance between the ease of business operations and the level of information security. Although all organizations should promote the "do the right thing" principle and trust that their employees will follow it, they also need to monitor internal activity.

Recognizing internal threats as a risk and following a "trust but verify" approach are two big steps towards protecting against it.

Bibliography

[1] Common Sense Guide to Mitig at ing Insider Threats 4th Edition, 2012, CMU/SEI-2012-TR-012

[2] Protecting Against Insider Attacks, SANS Publication 2009

[3] US CERT Insider Threat Center publication

[4] J. Hunker and C. W. Probst, "Insiders and insider threats – an overview of definitions and mitigation techniques," Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, vol. 2, no. 1, pp. 4–27, 2011.

[5] C. Colwill, "Human factors in information security: The insider threat who can you trust these days?" Information Security Technical Report, vol. 14, no. 4, pp. 186–196, 2009.

[6] E. D. Shaw and H. V. Stock, "Behavioral risk indicators of malicious insider theft of intellectual property: Misreading the writing on the wall," Symantec, Tech. Rep., 2011.

DOI: 10.21279/1454-864X-17-I1-060