The Enemy You Know:

An Analysis of the Insider Threat

By Ted Harrington, Executive Partner, Independent Security Evaluators
June 2, 2015

INTRODUCTION

Many organizations are already cognizant of the fact that there are security threats originating from the inside, beginning with their own trusted employees and partners. However, many organizations do not necessarily differentiate between the various types of internal adversaries, and may also be unaware that a uniform defense posture is not effective, as different defense strategies are required to thwart each type of adversary. This article will analyze the different types of internal threat actors, and discuss how each is defended against. It will consider both technology and psychology solutions, and aim to do so in a way that is immediately actionable for organizations of all types.

THREAT MODELING

Any discussion of security strategies would be incomplete without an understanding of how those strategies relate to an organization's threat model. All companies *must* define their threat model, which effectively articulates assets, adversaries and architecture. When considering assets, the organization must understand not only which assets are worth protecting, but must also quantify those assets in terms of both the downside to the company *and* the potential upside to the adversary in the event of asset compromise. It is important to note that those two metrics are not necessarily the same. Once an organization understands the value of their assets, the organization can then clearly understand who the adversaries are that would be interested in attacking in order to compromise the assets. Once assets and adversaries are understood, the organization is then best able to articulate the defense architecture that is most effective.

ADVERSARIES

In order to fully understand internal adversaries, one must first consider external adversaries. In the context of most industries, there are four primary categories of external adversaries: Casual hackers are those motivated by notoriety; they steal content so they can brag about it and obtain credibility from their peers. Hacktivists, including groups such as Anonymous, attack in order to make political statements. Organized crime make business decisions, and steal assets in order to make money. Nation states attack to pursue geopolitical and economic interests.

When analyzing the difference between external adversaries and internal adversaries, it is important to remember that these terms are not opposite within this context; rather the difference between external and internal lies in conditions of trust and access. Internal adversaries could be extensions of the external adversaries discussed above, but they have additional trust and access typically granted to employees and other insiders. Internal adversaries are broken into three different types of actors: accidental, opportunistic, and determined. The defenses against these, by way of technology and psychology solutions, break down into prevention, deterrence, or mitigation.

ACCIDENTAL INSIDER

The accidental insider harms the company not with malicious intent, but simply as a result of poor decision making. Fundamentally, people are an organization's weakest link. People create weak passwords and reuse them across different services; people lack discretion when clicking links in emails or inserting random thumb drives; and people are notoriously susceptible to social engineering attacks. All of these conditions lead to otherwise trusted employees unwittingly turning into the accidental insider.

Organizations best defend against the accidental insider through prevention, whereby the organization mitigates damage in the event that the trusted insider unwittingly compromises assets. Encryption and multi-factor authentication are a few good examples of technology solutions that are effective in minimizing the damage done by the accidental insider. Training is an effective psychology solution against this type of adversary, whereby the organization helps its people become better educated about how their actions can deliver significant harm to the organization.

OPPORTUNISITC INSIDER

The primary defining characteristic of the opportunistic insider is the he or she will compromise an asset when there is no repercussion for doing so. The opportunistic insider may not initially set out to harm the company, rather over the course of performing his job duties he might be granted access to a valuable asset from which he may benefit by compromising, perhaps achieving financial gain by selling it or obtaining notoriety for being the first person to leak it. Without a disincentive in place, this employee may choose to pursue these gains.

Organizations can best defend against the opportunistic insider through deterrence. If this type of adversary thinks he will be caught, he is far less likely to compromise the asset. Logging, monitoring, and digital rights management are a few examples of technology solutions that are effective against this type of adversary, as such tools create a trail that leads back to the adversary. The most effective psychology solution against this type of adversary is awareness. It is important to make the distinction between training and awareness: while training seeks to educate employees about their individual actions, awareness seeks to galvanize the group of employees to protect assets together. If the opportunistic adversary thinks she is being observed by her colleagues, she is less likely to compromise assets.

A great example of this comes from psychologist Thomas Moriarty through his experiment colloquially referred to as the Beach Blanket experiment. In this landmark study of group dynamics, Moriarty researched how bystander involvement affects theft deterrence. His researchers found that when bystanders were asked to be involved in the protection of an asset, the instances in which they took action skyrocketed, stating that "results support the notion that prior commitment simplifies the decision process and produces a more responsive bystander." (http://files.eric.ed.gov/fulltext/ED076923.pdf) This premise readily applies to the concept of awareness, whereby teaching employees about how and why to be observant of their workplace, coworkers and assets will reduce the instances of attacks by the opportunistic insider.

DETERMINED INSIDER

The determined insider is the most dangerous category of internal adversary, because the determined insider is motivated to harm the company. There are two notable subgroups within this adversary category: disgruntled insider and malicious insider. The disgruntled insider has become dissatisfied with the company for reasons such as being passed over for a promotion or by becoming disillusioned with the corporate mission. The malicious insider is an agent for one of the external threats previously mentioned. What makes the determined insider especially dangerous is that because he is motivated by malice, the aforementioned technology and psychology solutions against the other internal adversaries are ineffective. For instance, the disgruntled insider knows what he is doing will harm the company but proceeds anyways, and so training and even awareness will not necessarily stop him.

Mitigation is the best defense against the determined insider, whereby the organization assumes the posture that the adversary has already compromised an asset and makes it difficult for the adversary to compromise additional assets. One effective solution against this type of adversary is separation of privileges. Through privilege separation, an organization reduces any particular user's privilege to the absolute minimum that still enables him to be successful in his role. When done properly, privilege separation sets up employee roles like a chessboard: a large number of weak user roles (pawns), a small number of semi-powerful management roles (rooks) and a very limited number of all-powerful admin roles (queen). By limiting the power of most roles, this decreases the likelihood that the determined insider adversary would be powerful. It is important for organizations to remember that even well-designed privilege separation must be implemented properly, in such a way that low level users are not able to escalate privileges into more powerful admin roles.

SUMMARY

The internal threat is a real adversary who can do significant damage to most organizations. By understanding the distinctions between the different types of internal adversaries, organizations can design and implement an effective suite of defenses to counter each type of foe.

About the Author

Ted Harrington is Executive Partner and co-owner of Independent Security Evaluators, the elite organization of security researchers and consultants most commonly recognized for being the first company to hack the iPhone. He drives thought leadership initiatives for ISE, and he is one of the founding leaders of DEF CON's IoT Village. Mr. Harrington was recently named 40 Under 40 in the 8th largest city in the United States, where he was not only one of the youngest members of the class but also was the only honoree from the field of information security. He holds a bachelor's degree from Georgetown University.