Attivo NETWORKS®

Effectively Defend Against Insider Threats

Insider threats took center stage in 2017, and so far in 2018, there does not appear to be any indication that trend will slow down. While most of the attention is focused on external threats, nation-state attacks, and ransomware, it is increasingly important for organizations to be able to identify and stop attacks from within. Whether these threats are from employees, contractors, or suppliers, insider threats start with the advantage of already being inside—often with privileged access to the network and sensitive information.

Despite knowing of the risk of insider threats and increasing evidence of the damage that they can inflict, most organizations are not adequately prepared to detect or prevent such attacks. The primary focus of most computer and network security efforts is to keep bad guys outside the network from gaining access and getting inside. While that is certainly important, the reality is that the potential damage from insider threats is a much larger risk.

Deception technology can effectively protect sensitive assets and data from an insider threat—and it doesn't require profiling or user behavior tracking or analysis to uncover a threat.

Attacked from Within

An insider threat is a threat caused by an authorized user with permission to access sensitive servers or data. By virtue of being a trusted user with access to the network, they are in a position to compromise, expose, or steal information. There are many possible motives behind why a user might leak or compromise data: They may wish to make a point or get revenge. They might be planning on leaving the company and want to take customer data or intellectual property with them. In many cases, it is simply a crime of opportunity—curious employees poking around where they shouldn't be and accessing servers, applications and data they normally wouldn't. Insider threats can also come from trusted third parties—contractors, suppliers, or partners who have been granted access to your network or sensitive data.

According to a report from Beazley, 30 percent of the breaches from the first six months of 2017 were the result of either employee error, or data breached while controlled by third-party suppliers. A separate study by Soha Systems found that 63 percent of all data breaches are linked—either directly or indirectly—to third-party access. A survey conducted last fall by the Ponemon Institute revealed that 56 percent of organizations have suffered a data breach of some sort that was caused by one of their third-party vendors.

Even in the case of an outside attacker, though, many attacks start by phishing or stealing valid user credentials to gain access to the network. From a security and data protection standpoint, these still appear to be insider attacks as well and effective detection and prevention of such activity could help avoid these attacks.

The following cases illustrate why organizations are turning to deception technology for early visibility of insider threats:

Edward Snowden / Bradley (Chelsea) Manning

Edward Snowden was a contractor working for the NSA. Bradley Manning was a soldier in the US Army. In both cases, these individuals were authorized users with access to sensitive information and they each made a conscious decision to exfiltrate terabytes of classified data and leak it to the world to make a statement.

Texas Lottery

An employee at the Texas Lottery Commission copied the personal information of more than 100,000 individuals onto computer disks. He captured names, addresses, Social Security numbers, and lottery prize amounts of the victims—claiming that he wanted to retain it for possible future reference as a programmer at other state agencies.

New York State Electric & Gas

In 2012, an inside attacker compromised the Social Security numbers, birth dates, and some personal account information of nearly 2 million customers of New York State Electric & Gas and Rochester Gas & Electric. A contractor working for a software consulting firm doing work for the parent company of both utilities gained unauthorized access to the customer databases.

Target

One of the most high-profile data breaches in recent memory was Target. The retail giant was hit by an attack that compromised credit card information and personal data of up to 100 million customers. By hacking a third-party contractor and gaining trusted access to the Target network, attackers were able to move freely across the Target network environment and capture credit card data, encrypted PINs, names, addresses, phone numbers and email addresses.

Verizon

Verizon suffered a data breach that exposed six million customer records. The actual breach, however, was caused by a third-party customer service analytics vendor, Nice Systems. Nice Systems stored six months of customer service call logs—including account and personal information of the Verizon customers—on a poorly configured Amazon S3 storage server that was exposed to the public.

Equifax

The biggest data breach of 2017 was Equifax. The credit monitoring company suffered a breach that exposed sensitive personal information, including names, Social Security numbers, birth dates, addresses and driver's license numbers of millions of customers. The data breach occurred thanks to a serious security flaw in Apache Struts and a malicious download link on the Equifax website from a third-party vendor.

Risk of Insider Threat

Insider threats are more insidious than external attacks in many ways. One of the biggest problems with effectively detecting and identifying insider threats is that the insider generally has the benefit of authorized network access. The activity seems normal—especially for insiders authorized to access sensitive data. It is difficult to determine intent or separate normal activity from suspicious or malicious behavior. Tools that attempt to detect insider threats by profiling users or monitoring and tracking behavior can result in lower employee morale. These programs also often result in the late discovery of threats and—in some cases—may be a violation of the user's privacy.

Because insider threats have permission to be on the network and have authorized access to sensitive data, they can go undetected for months—or even years—spreading laterally throughout the network and poking around in search of sensitive data. Attackers with insider access also generally have the means to cover their tracks or erase evidence of their presence.

Detecting Suspicious / Malicious Insider Activity

The challenge, then, is how does an organization effectively detect and identify suspicious or malicious insider activity? Monitoring for suspicious or anomalous behavior is one approach—but it's susceptible to delays in threat discovery, as well as misleading results or false positives. For example, a security solution could detect activity on a Saturday from an employee who typically does not access the network over the weekend and flag it as anomalous behavior, but it's possible the employee just needed to get some work done over the weekend. Sifting through the noise and separating actual threats from false positives increases complexity and creates additional tasks for IT staff who are generally maxed out as it is.

> 56 percent of organizations have suffered a data breach of some sort that was caused by one of their third-party vendors.

There are, however, some things an organization can watch for that would be a clear indication that something suspicious or malicious is going on that needs attention:

- Attempts by authorized users to access servers or data they shouldn't be.
- Authorized users accessing or requesting access to information that is unrelated to their roles or job duties.
- Theft of authorized user credentials.

Whether the activity is from an authorized employee just poking around where they shouldn't be out of curiosity, an authorized employee with malicious intentions accessing servers or data to cause damage or steal information, or an external attacker that has obtained valid credentials of an authorized user, if any of these activities are detected it is cause for alarm.

Thwart Insider Attacks with Deception Technology

Deception technology is the quickest and easiest way to detect suspicious or malicious activity from insiders. The "3 D's" of deception technology—deceive, detect, and defend—ensure that IT security personnel can effectively identify and thwart insider attacks without increasing complexity or adding unnecessary noise.

Deceive

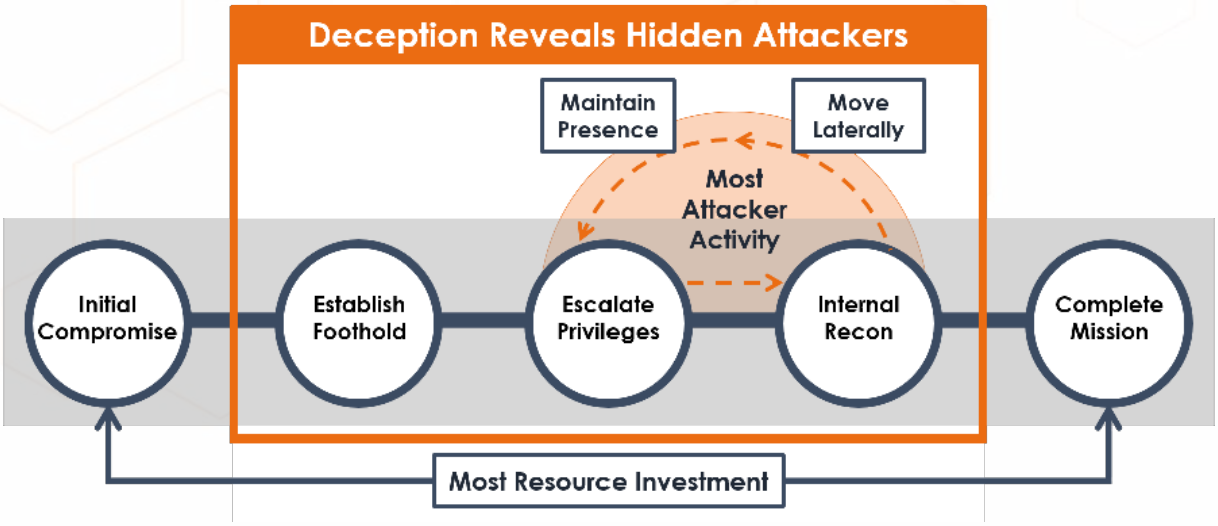
The first—and arguably most important—pillar of deception technology is to deceive attackers. Most attackers either scan the network in search of hosts with services or applications to compromise, or they seek vulnerable endpoints to steal employee credentials and data. Deception servers and lures act as attractive bait designed to entice attackers into engaging.

Deception technology doesn't require signatures or agents to run on an organization's servers or endpoints. It relies on a matrix of authentic decoys—servers, endpoints, and applications—that have the characteristics attackers are looking for.

Detect

Deception technology provides early and efficient attack detection across a wide range of potential threats and attacks. Using a comprehensive array of virtual machines, IP services, and subnets, deception technology gives visibility across a broad and evolving attack surface. Deception technology can detect attacks in the network, data center, cloud workloads, IoT devices, SCADA, POS, router, and more.

As attackers attempt to conduct reconnaissance or move laterally through the network or seek out endpoints to extract credentials, they will engage with deception decoys and reveal themselves. Deception technology provides an effective means of detecting insider threats, as well as advance external or third-party threats, malware or ransomware attacks, or access by attackers using stolen user credentials.



Defend

Once the attacker has taken the bait and the deception solution has detect the threat, the next step is to take action to thwart the attack and defend the network and data. Deception technology arms an organization with substantiated threats and alerts that leave no room for doubt that there is suspicious or malicious activity.

The Attivo ThreatDefend™ Platform conducts a detailed automated analysis of malware and phishing attacks. It also enables integration with various platforms and security solutions and arms the security team with playbooks to automate deployment, blocking, and quarantine activities when it detects a threat.

Prove

There is also a fourth thing above and beyond the "3 D's" –a "P" for "prove". Deception technology provides the forensic evidence necessary to prove that the insider attack occurred. Once it detects a threat, it monitors and records the activities to provide comprehensive forensic reporting and an ability to drill down and analyze details of the attack.

With Attivo deception technology, an organization can quickly identify policy violations and actions ranging from simple things like employees taking shortcuts, to more nefarious behaviors like actual attacks or compromise. The forensic evidence collected by deception technology provides detailed tracking of the attacker's actions and gives HR and Legal the proof necessary to act.

Conclusion

Technology continues to evolve, but so do attackers and the threat landscape. Attackers continue to develop new attacks. The simple truth is that there is absolutely no way to prevent 100 percent of attacks—and that is especially true when the attacker has the benefit of being an insider with authorized access to network resources and sensitive data.

Regardless of whether the attacker is a disgruntled or financially-motivate employee, a contractor or supplier, or an external actor using compromised credentials, there are certain actions that are common to all attacks. The attacker must conduct some reconnaissance of the network, establish a foothold, and access sensitive data—and that is a phase of the attack life cycle that is often ignored or underinvested in. Attempts to analyze log data or monitor for anomalous behavior create added complexity and are plagued with false positives.

Deception technology is a tried-and-proven technique for outmaneuvering the adversary. Applying deception technology provides the tools an organization need to quickly and accurately detect and identify suspicious or malicious insider activity. More importantly, it provides the proof needed to take decisive and substantiated action.

About Attivo Networks

Attivo Networks® is the leader in dynamic deception technology for real-time detection, analysis, and accelerated response to advanced, credential, insider, and ransomware cyber-attacks. The ThreatDefend Deception and Response Platform accurately detects advanced in-network threats and provides scalable continuous threat management for user networks, data centers, cloud, IoT, ICS-SCADA, and POS environments. www.attivonetworks.com