INSIDER THREAT: DETECTION, PREVENTION AND RESPONSE

INSIDER THREAT:

Detection, Prevention and Response

Roughly 50 percent of organizations in 2012 experienced at least one event due to insider threat, according to Carnegie Mellon's CERT.

- About 20 percent of incidents studied in the 2015 Verizon DBIR were the result of inside threats.
- Insider threat events are assumed to be underreported because they are often managed internally. [3]

A Number of High Profile Incidents Over the Years

Insider incidents may be less frequent than other types of events, but their impacts are more severe, and motivations are diverse. Malicious insiders can choose to attack for espionage, financial gain or simply to do damage in pursuit of personal goals. Carnegie Mellon found that 53 percent said those incidents had a worse impact than those perpetrated by outsiders. [4]

- The public and damaging release of classified information by PVT Manning in 2010 and Edward Snowden in 2013 raised awareness everywhere about the weakness of high-security systems to adversarial insiders. [5]
- In 2013, an employee of the Korean Credit Bureau stole the personal and financial data of 20 million consumers to sell to marketing firms. [6]
- Also in 2013, retailer Target announced that customer data was breached due to compromised credentials of a legitimate third-party contractor. [7]
- In August 2015, hackers publically released a large volume of user data associated with Ashley Madison. [8] [9] Ashley Madison's leadership attributed the attack in part to a third-party with internal access to the network. The attack exposed personal data of more than 30 million users.

THE PATH FORWARD:

Evolving with Attacks

The most advanced insider threat programs leverage threat modeling to better understand their threats. To mirror this approach, begin by looking at the key revenue-generating processes and assets in the enterprise. Then, model these chains of events to focus mitigation efforts. [10] Thwart the attack path by aligning people, process and technology.

An insider threat is an employee, contractor or other trusted party with legitimate network access that harms an enterprise's finances, reputation or clientele, or takes actions that are contrary to policy, regulation or law.

People: *a range of essential internal and external expertise*

Professional staff handle developing preventative controls, early detection controls and response controls. The preventative security expertise needed is broad and includes: fraud, investigation, forensics, identity and access management, privileged identity management, asset management, SDLC management, training and awareness management as well as behavioral reporting and modification.

Expertise in fraud prevention is a key resource that comes into play before attacks even get started. First, assess how you link your own staff with external expertise. Security practitioners with an eye towards fraud prevention need to build tight linkages with forensics and systems auditing teams. For example, security personnel need to be aware if IT audit teams are checking that access to resources is appropriate to the user roles, that administrators are maintaining separation of duties, and that provisioning and de-provisioning happens accurately and quickly.

Second, try to pull in external expertise more closely to the problem. If you are a research organization, consider asking for a data scientist to help tailor your anomaly monitoring tools. If your enterprise has access to accounting talent, ask those with forensic accounting experience to help you hunt for fraudulent insiders.

Technical expertise is needed to maximize tools and to incorporate incident response functions. Tight integration among players during incident response requires practiced coordination and often outside help. This can include MSS providers, forensic teams or table top facilitators.

The insider threat team should also work closely with internal HR, legal and finance for multiple reasons. For example, HR often maintains the most updated contextual employee data and may be aware of future negative workforce events. These groups will also more fully understand the policy implications of the insider threat program.

Processes: *understanding internal operations and hardening the attack path*

Understanding your current processes and associated assets is widely agreed to be one of the most important steps a security team can take, but the assessment is hard to complete.

Instead of getting bogged down in trying to gain complete awareness, start by identifying the key revenue generating processes and associated assets to the business as a whole. Categorize assets within those processes and understand the value they represent. For example, if there is intellectual property that gives the company a competitive advantage, critically assess what systems is the data on, who has access and how might the IP be stolen? If the concern is about financial assets, what fraud schemes might work well, and how might you identify those actions?

Once these processes and their weaknesses are understood, look to the likely insider threats in your environment. Compare the capabilities of these potential insider attackers to the weaknesses in your key processes to determine your exposure.

Make sure to assess the threat by considering different insider kill chains. The security team can model the threat by examining the problem using the kill chain—looking for opportunities to predict, prevent, detect, respond and recover from an incident. The program steps to fulfill these requirements are summarized below.

To address the early stages of the attack, **prevent** insider threat incidents by educating the workforce on what to look out for, deterring inappropriate actions with consistent sanctions, and stop completion of the attack with technical controls.

To improve **detection** during the reconnaissance and packing stages of an attack, consider adding hunting capabilities to your security program. Make sure that monitoring tools such as user behavior analytics (UBA) and data loss prevention (DLP) are tailored to your specific environment.

Incident **response** processes are vitally important and branches of the process should be tailored to insider threats. Insider threat incidents are usually more damaging and there are often HR implications. The potential impact of these incidents demands a broad team of expertise.

This comprehensive response team will most likely include legal, HR, compliance and possibly privacy teams. Establishing a broad team can be at odds with the need to limit the number of employees involved in the investigation of an insider. Explicitly prepare methods for keeping the investigation confidential in both your processes and tools.

Insider threat program managers should continually ensure that their investment link back to evolving strategic goals created by the CISO is in conjunction with senior risk management. Program managers should also be tightly linked with incident response functions to make sure that their assumptions about current threats are kept fresh.

Technology: *solutions that enhance detection, prevention and response*

Technology solutions capable of enhancing prevention, detection and response to insider threats cover the entire spectrum of potential security investment. All of the following can be used: identity and access management (IAM), identity governance and administration (IGA), privileged identity, account and user management (PIM, PAM, PUM), security incident and event management (SIEM), end point monitoring, user behavior analytics (UBA) and data loss prevention (DLP).

Investment should be aligned with the maturity of your program and the problem you are trying to solve. Solutions research teams can aid in providing a fresh look at your program and the appropriate tool for the job. [11] [12] [13] [14]

Measurement: *walk before you run*

The initial Key Performance Indicators (KPIs) that measure the effectiveness of this program can primarily be drawn from incident metrics that describe the initial attacker. Organizations should collect incident metrics, making the incremental maturity of improving coding about the originating attacker achievable. With this incident data, the ability of the program to reduce insider-generated incidents can be tracked over time.

The next level in maturity for measurement should be Key Risk Indicators (KRIs). These are indicators that can give early warning that an attack is either taking place, or about to take place. For example, seeing multiple data access anomalies by a fully authorized user could be an indicator of an inside attack. These sorts of KRIs eventually should become rules that drive automated detection efforts.

Once this is accomplished, the more difficult task of monitoring cost associated with insider fraud can be measured over the life of the program. The program should be able to point to a decrease in the amount of insider fraud and insider generated incidents in order to claim it is having a measurable impact on outcomes.

CALL TO ACTION

Insider threat program managers need to create organizational linkages that incorporate a broad array of security functions. This will prevent reinvesting in functions that already exist in the enterprise. Managers need to actively assess the capabilities of their current tool set and decide whether to invest in maturing those tools or in purchasing new ones.

Having a well-thought out strategy based on an integrated functional model will take more time up front, but will help orchestrate the many moving pieces required to ensure success. Protecting against insider threats is essential to insulating the enterprise from the most damaging incidents, and preserve mission-critical processes.

Verizon DBIR years 2009 to 2015, DBIR 2015 Figure 3 and personal email from DBIR author.

Carnegie Mellon Cert. "Insider Threat: How Bad Is It?" Carnegie Mellon Cert. 2013. Retrieved from: http://resources.sei.cmu.edu/asset_files/Presentation/2013_017_101_58739.pdf

Carnegie Mellon Cert. "Insider Threat: How Bad Is It?" Carnegie Mellon Cert. 2013. Retrieved from: http://resources.sei.cmu.edu/asset_files/Presentation/2013_017_101_58739.pdf

Carnegie Mellon Cert. "Insider Threat: How Bad Is It?" Carnegie Mellon Cert. 2013. Retrieved from: http://resources.sei.cmu.edu/asset_files/Presentation/2013_017_101_58739.pdf

Sternstein, Aliya, "Watchdog Says Pentagon Needs to Crank Up Insider Threat Monitoring." June 4, 2015. Retrieved from: http://www.nextgov.com/cybersecurity/2015/06/watchdog-says-dod-needs-crank-insider-threat-monitoring/114430/

AFP. "20 Milllion People Fall Victim to South Korean Data Leak." AFP. January 19, 2014. Retrieved from: http://www.securityweek.com/20-million-people-fall-victim-south-korea-data-leak

Krebs, Brian. "Email Attack on Vendor Set Up Breach on Target." Krebs on Security Blog. February 14, 2014. Retrieved from: http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/

Krebs, Brian. "Online Cheating Site AshleyMadison Hacked." July 15. Retrieved from: http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/

Avid Life Media. "Statement from Avid Life Media, Inc." July 20. Retrieved from: http://media.ashleymadison.com/statement-from-avid-life-media-inc/

Cappelli, Dawn, Moore, Andrew, and Trzeciak, Randall. "The CERT Guide to Insider Threats." Boston. 2012.

Wind River. "Security in the Internet of Things: Lessons from the past to secure the future." Wind River. January, 2015. Retrieved from: http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf

Verizon Research. "State of the Market: The Internet of Things 2015." Verizon. p.20.

Intel. "Intel Announces Expanded Choices in Silicon and Software for Gateways." Intel. Retrieved from: https://www-ssl.intel.com/content/www/us/en/embedded/solutions/iot-gateway/overview.html

IoT Analytics. "The Top 20 Internet of Things Companies Right Now." IoT Analytics. February 24, 2015. Retrieved from: http://iot-analytics.com/20-internet-of-things-companies/

1125 17th Street, Suite 1700
Denver, CO 80202

800.574.0896 | www.optiv.com

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.

10.15 | F1