International Center for Enterprise Preparedness (InterCEP)

Insider Threat by Cyber Vector

Web Forum

On January 29, 2019, **Randall Trzeciak**, director of the ***CERT Insider Threat Center*** at ***Carnegie Mellon University's Software Engineering Institute***, discussed insider threat by cyber vector. As part of the discussion he described different types of insider threats, trends in insider threat detection, best practices on insider threat mitigation, and strategies for building an effective insider threat program.

Introduction

CERT's definition of insider threat is: "The potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization."

Examples of insider threat incidents that resulted in damages to organizations include:

- A recently demoted software engineer that stole over $1 billion worth of technology and went to work for a foreign competitor
- A former Information Security Director at a Lottery Association used Rootkit to alter a random number generator which allowed accomplices to win $14 million
- A disgruntled contract employee at a wastewater facility accessed the company's SCADA systems after termination using a company laptop that was not returned and released 800,000 liters of sewage

Could something like this happen to your organization? Could someone steal your technology and intellectual property? Can these incidents be prevented from happening? There are common patterns around insider incidents that allow organizations to integrate this threat to their risk management strategies.

CERT collects and shares incident data and through collaborative agreements can also provide services related to querying the incident database to examine impacts related to the most common types of insider threats.

Mitigating Insider Threats and Incidents

Actions to prevent insider incidents that can cause harm intentionally or unintentionally include:

- Identifying potential insider threats, which can include anyone who has access to an organization's assets, including full-time and part-time employees (current or former if they retain access), sub-contractors, supply chain, etc.
- Identifying the potential impacts of individuals that have access to an organization's systems and assets
    - What could an insider risk mean for an organization's operations, finances, or health and safety?
- Incorporating employee assistance programs may deter some employees from moving in the direction of becoming insider threats

CERT has developed a ***best practice guide*** (see Additional Resources section) that includes steps to follow to create an Insider Threat Program that can help organizations to identify threats and to mitigate this organizational risk.

An organization's Insider Threat and Risk Program may look different from those used by government agencies or other industry organizations in different sectors.

Risk Indicators

Risk indicators include:

Organizational risk indicators: events or actions or conditions that might incentivize insiders to do harm, as well as behavioral violations, absenteeism and tardiness.

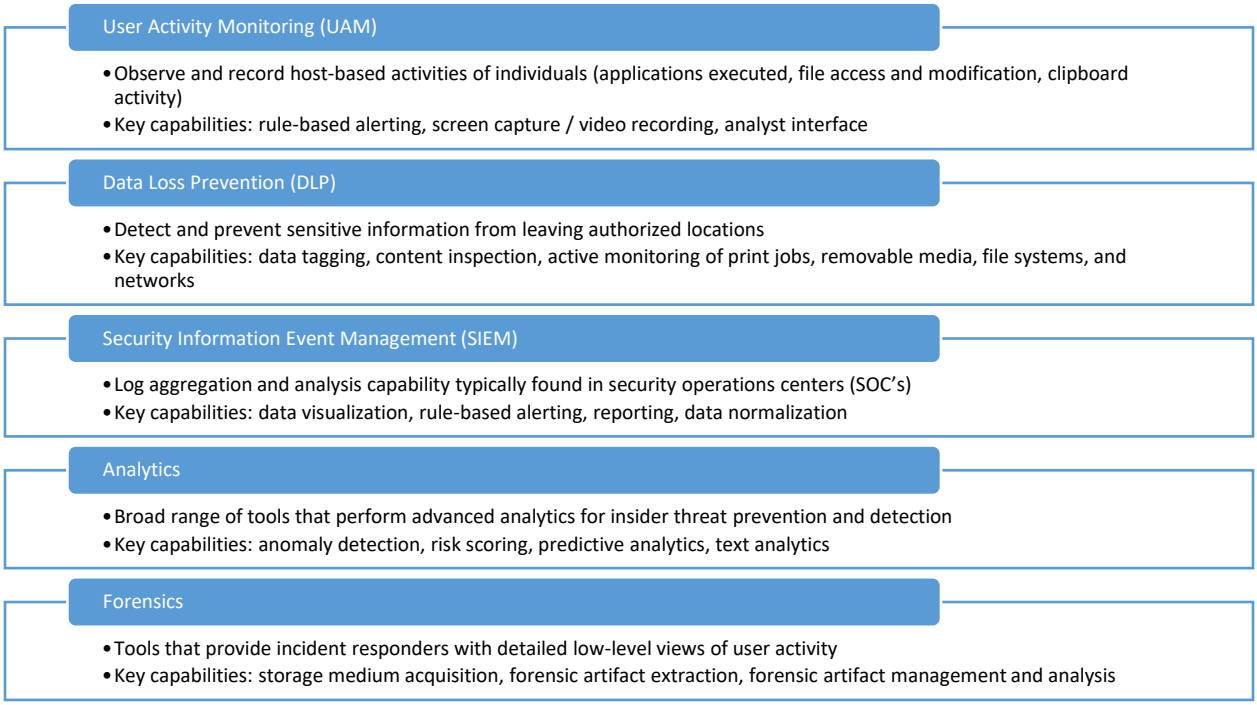
When these signs are present, they can be moved away from a path that will result in harm. The goal is to identify these characteristics. Network probing may help in this area.

Other indicators that can be considered include:

- Physical security access logs
- Obtaining clearances
- Data from a SOC - SOCs are typically focused on external threats but monitoring for insider threats can also be incorporated into their activities

Figure 1 summarizes the tools that are available to detect and prevent insider threat incidents.

Figure 1. Tools for Detecting and Preventing Insider Incidents



Source: CERT

Q. Can this be integrated with other elements of HR and others that can raise flags?

Information technology is a strong component of an insider threat program. Behavioral detection tools and analytic tools can be integrated into HR, physical security, and other departments that can do some user activity monitoring.

Types of Insider Incidents

There are three categories of malicious insider incidents:

- IT sabotage
- Fraud
- Theft of intellectual property

In addition, there are four basic categories of non-malicious insider incidents:

- Unintentionally publishing or disclosing information
- Fishing or social engineering that trick employees to allow access to networks
- Improper protection of physical data – inadequate disposal
- Losing laptops or cell phones that are not encrypted or that were inappropriately shut down

Building an Insider Threat Program

An insider threat program should include the following aspects:

- Data loss prevention
    - Email filtering
    - White listing and black listing web pages for external threat mitigation can also prevent/deter insider threat
- Intrusion prevention

This is the foundation of a program but it should not be limited to this. It is important to integrate human resource data and physical security data.

CERT's recommended best practices for insider threat mitigation are summarized in Table 1.

Table 1. Recommended Best Practices for Insider Threat Mitigation

1 - Know and protect your critical assets.	11 - Institute stringent access controls and monitoring policies on privileged users.
2 - Develop a formalized insider threat program.	12 - Deploy solutions for monitoring employee actions and correlating information from multiple data sources.
3 - Clearly document and consistently enforce policies and controls.	13 - Monitor and control remote access from all endpoints, including mobile devices.
4 - Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.	14 - Establish a baseline of normal behavior for both networks and employees
5 - Anticipate and manage negative issues in the work environment.	15 - Enforce separation of duties and least privilege.
6 - Consider threats from insiders and business partners in enterprise-wide risk assessments.	16 - Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.

7 - Be especially vigilant regarding social media.	17 - Institutionalize system change controls.
8 - Structure management and tasks to minimize unintentional insider stress and mistakes.	18 - Implement secure backup and recovery processes.
9 - Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.	19 - Close the doors to unauthorized data exfiltration.
10 - Implement strict password and account management policies and practices.	20 - Develop a comprehensive employee termination procedure.

Source: CERT.

A resource for organizations that are considering implementing an insider threat program is the roadmap available on the Intelligence and National Security Alliance (INSA) web page (see the Additional Resources section). This roadmap discusses how to initiate a program, the planning stages, how to sustain buy-in, and how to integrate it with enterprise wide risk management programs.

The National Insider Threat Task Force also has guidance and guidelines for federal government agencies that include cost estimates for building an insider threat program and maturity models (see the Additional Resources section).

An insider threat program will evolve over time. During the first two years the program might focus on identifying a period of risk for departing employees, and then evolve to work with human resources to identify potential risks, learn when people announced they were leaving, and examine data use/download/access as they leave, as well as email access on the organization's network.

There is not one tool that can detect all insider threats and prevent and deter these incidents. It is best to start small and improve over time, small wins will allow an organization to achieve success and gain support from senior management.

A key aspect of an insider threat program is to compare technical and behavioral anomalies. An example is to use a 30 day rule – about 80% of individuals who do harm do it within 30 days of announcing they are leaving. It is important to conduct advanced monitoring during this period.

Additional Resources:

- CERT Insider Threat Center at Carnegie Mellon University's Software Engineering Institute: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=91513
- CERT Insider Threat Center, Cybercrime Survey Collection: https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=484019

- Software Engineering Institute at Carnegie Mellon University: http://www.sei.cmu.edu/
- Collins, M., Theis, M., Trzeciak, R. F., Strozer, J., Clark, J., Costa, D., Cassidy, T., Albrethsen, M., & Moore, A. P. (2016). Common Sense Guide to Mitigating Insider Threats (5th Ed.). Pittsburgh: Software Engineering Institute. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=484738
- Moore, Andrew; Savinda, Jeff; Monaco, Elizabeth; Moyes, Jamie; Rousseau, Denise; Perl, Samuel; Cowley, Jennifer; Collins, Matthew; Cassidy, Tracy; VanHoudnos, Nathan; Buttles-Valdez, Palma; Bauer, Daniel; & Parshall, Allison. The Critical Role of Positive Incentives for Reducing Insider Threats. CMU/SEI-2016-TR-014. Software Engineering Institute, Carnegie Mellon University. 2016. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=484917
- The CERT® Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud) (SEI Series in Software Engineering) by Dawn M. Cappelli, Andrew P. Moore and Randall F. Trzeciak. 2012. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=30310
- Intelligence and National Security Alliance (INSA) – Insider Threat Program Roadmap: https://www.insaonline.org/insider-threat-roadmap/
- National Insider Threat Task Force: https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf