International Center for Enterprise Preparedness (InterCEP)

Insider Threat by Cyber Vector: Briefing and Key Deterrence Strategies

Web Forum

On March 16, 2016, 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 malicious insider threats, key research efforts in this area, best practices to mitigate this type of threat, and strategies for building an effective insider threat program.

The CERT Insider Threat Center

The CERT Insider Threat Center has been working with the U.S. Secret Service since 2001. Its mission is to enable effective insider threat mitigation, incident management practices, and develop capabilities for deterring, detecting, and responding to evolving cyber threats. The Center conducts research and outreach on behalf of the federal government to address insider threats.

Insider Threat

Insiders are individuals with authorized access to data, systems and networks. Because of their position they are in, they may be able to bypass security measures through legitimate means. Examples of individuals that could pose an insider threat include current or former employees, contractors, or other business partners. Former employees may pose a threat if they were granted authorized permission to access networks and data and such permissions are not taken away when they leave.

Individuals become a threat when they have or have had authorized access to an organization’s network, systems, or data, and when they intentionally exceed or misuse that access in a manner that negatively affects the confidentiality, integrity, or availability of the organization’s information or information systems.

The threat is to an organization’s critical assets, which may include people, information, technology and facilities. The impacts are to the confidentiality, availability and integrity of these critical assets. The form of the threat depends on the motivations of those who perpetrate it.

Examples of insider threat incidents include:

- 911 information technology services were sabotaged in four cities by a disgruntled employee
The SCADA systems of a wastewater treatment plant were sabotaged by a disgruntled contractor resulting the release of 800,000 liters of raw sewage

A disgruntled system administrator deployed a logic bomb and modified the system logs to frame his supervisor – this happened even though the administrator had been demoted and his privileges should have been restricted

A research scientist downloaded thousands of documents containing his company’s trade secrets before going to work for a competitor

A ring of DMV employees sold more than 200 fake licenses for more than $1 Million

There are different types of insider threats, and these include:

- Insider information technology sabotage
- Insider theft of intellectual property
- Insider fraud
- National security espionage

Insider threats can also be non-malicious in intent. Examples include:

- Accidental disclosures of information through the Internet and social media
- A person in an organization is the victim of malicious code, such as phishing email attacks, malware and/or spyware
- Sensitive information is improperly discarded
- Data storage and other devices are lost, improperly discarded or stolen

**Insider Threat Data**

The CERT Insider Threat Center has 1,300 incidents in its insider threat incident database. These incidents are from publicly available information and go back to 1996. The data are available by sector. A challenge in terms of research in this area is that Insider incidents are underreported.

A 2015 survey attempted to address the prevalence of insider threats. The results suggested that since 2004 about 50% of respondents experienced at least one insider malicious incident every year. This survey is available on the CERT Insider Threat Center web site (See Additional Resources below).

A second interesting statistic relates to what organizations do when they find an incident. Over 75% of incidents are handled internally without any reporting or involving the law. As a result those who harm an organization in this way are typically not prosecuted. This poses a challenge because it means that background checks are not likely to capture such incidents for potential employees since there is no
record of them. The reason why most of these incidents are not prosecuted include lack of evidence, insufficient damages, and concerns about liability, reputational damage and negative publicity.

**Strategies to Mitigate Insider Threat**

It is important to understand that strategies to mitigate insider threats are not strictly technological in nature. The behavioral component is critical and if an organization ignores this aspect, it may be too late to avert an insider threat. Independent behavioral psychologists can provide key insights to an organization in terms of some of the motivating factors and conditions that are early warning signs for progression along a path to commit harm to an organization. Hence, solutions that incorporate both social/behavioral and technological components to identify someone on a path to cause harm, whether intentional or unintentional, are likely to be most effective.

As part of a strategy to address insider threat, an organization should learn from actual incidents and raise awareness about the kinds of behavioral and social traits in individuals that may suggest they pose a threat. Examples of behavioral traits in individuals who have posed a threat include lying in pre-screenings, a history of drug use and consistent complaining about tasks/jobs.

**Implementing an Insider Threat Program in Your Organization**

What department in an organization should be involved in an insider threat program? Most companies would say the IT department should handle insider threats. But this issue is broader than that. An organization should involve legal counsel and privacy officers when monitoring employees and contractors to ensure that privacy considerations are taken into account. Human Resources is very important if the strategy involves obtaining information about employees. Figure 1 shows how broad the key components of an effective insider threat program should be.

Three pillars of robust strategies include:

- Accurately measure trust
- Right size permissions for accessing assets
- Conduct effective monitoring (again including behavioral/social and technical aspects)

A core component of an insider threat program is the ability to collect and analyze data in order to identify indicators of potential insider activities. This can be accomplished by creating a data analytic hub that considers, for example, the physical side of data, behavioral analytics, co-worker reports and job transfers.
Figure 1. CERT Insider Threat Center Key Components of an Insider Threat Program

Source: CERT Insider Threat Center, Carnegie Mellon University.

Key insights from the web forum discussion included:

- Make sure you know what you are trying to protect
- Start with what you are doing today and what tools you have today and how they may be slightly retooled to address insider threats
- Do not neglect behavioral aspects - behavioral observables are usually available first before individuals with access/permissions decide to do technological harm

Guidance for designing an insider threat program are included in the report *Common Sense Guide to Mitigating Insider Threats*, 4th Edition (see Additional Resources below).

Additional Resources:


The International Center for Enterprise Preparedness (InterCEP)
New York University
Email: intercep@nyu.edu
Web: http://www.intercep.nyu.edu
• Software Engineering Institute at Carnegie Mellon University: http://www.sei.cmu.edu/
• Insider Threat Blog: http://www.cert.org/blogs/insider-threat/