Using Empirical Insider Threat Case Data to Design a Mitigation Strategy

Dawn M. Cappelli
Technical Manager, Threat & Incident Management
CERT Program, Software Engineering Institute
412.298.0532

dmc@cert.org

Categories and Subject Descriptors
A. General Literature; A.2 REFERENCE

General Terms
Security

Keywords
Insider Threat, Security, Technology, Mitigation

1. Understanding the Complexity of Insider Threat

According to research by the CERT® Program (CERT) in the Software Engineering Institute at Carnegie Mellon University, approximately half of all organizat1ons experience at least one electronic crime perpetrated by an insider each year.[1] These crimes include theft, sabotage, fraud, and espionage. CERT began researching this problem in 2001. It has compiled a database of more than 500 criminal cases in which current or former employees, contractors, or business partners abused the trust and access associated with their positions. As part of its research, CERT interviewed many victim organizations. It also interviewed some perpetrators themselves, complementing a wealth of case data with first-hand insights into the methods and motivations behind these crimes.

CERT researchers also collaborated with noted psychologists and others from the United States Secret Service, the FBI, and the Department of Defense to uncover key technical, social, and organizational patterns of insider behavior. Building on this work, CERT researchers constructed insider threat models using system dynamics techniques. These models suggest both the evolution of the threat over time and possible mitigation strategies.

Armed with insights from detailed case analysis and modeling, the Insider Threat Center at CERT is developing practical mitigation strategies organizations can implement to safeguard their critical infrastructure. Because of the complexity of the insider threat

problem, these strategies involve security officers, information technology staff, management, data owners, software engineers, and human resources personnel. Countermeasures include policies, practices, and technologies that focus on prevention, detection, and response.

One essential component of insider threat mitigation is an understanding of the complexity of this problem across the organization. While automated detection methods are the ultimate goal, CERT's research shows that most insiders carry out or set up their attack using authorized access and performing the same types of online actions they perform every day. Superficially, their malicious activities do not look any different from their everyday online activity. Thus, the design of an automated detection method presents a difficult problem. Therefore, CERT recommends a combination of technical methods and organizational processes for recognizing and communicating suspicious insider actions, events, and conditions to the appropriate personnel.

1.1 Detecting and Mitigating Specific Types of Insider Crime

CERT defines *Insider IT Sabotage* as an insider's use of IT to harm an organization or an individual. These crimes are usually committed by disgruntled system administrators or database administrators. They often destroy data or disrupt business operations. These crimes are frequently committed following termination and involve illicit access methods, such as backdoor accounts, malicious code, or passwords obtained through password crackers or social engineering. Often, insiders take technical actions prior to termination to provide access to carry out their attack following termination. Therefore, mitigation strategies include detection of configuration changes, perimeter controls to alert on suspicious traffic, and monitoring for unauthorized accounts. They focus on detection of unknown access paths prior to termination.

Insider Theft of Intellectual Property (IP) is an insider's use of IT to steal IP from the organization. This category includes industrial espionage. These crimes are usually committed by scientists, engineers, and programmers who steal assets they created: engineering drawings, scientific formulas, and source code, for example. CERT's research shows most insiders steal IP within 30 days of resignation. Therefore, an organization should consider policies and procedures that identify its most critical IP and include proactive logging of downloads, email, printing, file transfers, and timely auditing of those logs when an insider with access to the organization's critical IP resigns. Effective detection of information exfiltration relies on a comprehensive logging strategy combined with consistent auditing upon resignation by key personnel.

Insider Fraud includes crimes in which an insider uses IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or theft of information that leads to identity theft . These crimes

[1] http://www.cert.org/archive/pdf/ecrimesummary10.pdf

InsiderThreats'10, October 8, 2010, Chicago, Illinois, USA.
Copyright 2010 ACM 978-1-4503-0092-6/10/10.

are usually committed by low-level employees, such as customer support or help desk employees, using authorized access to systems. They often involve collusion with both outsiders and other insiders. A detection strategy for this type of crime involves monitoring insiders for non-work related activity and auditing database transactions for suspicious activity involving personally identifiable information (PII), credit card information, and other sensitive information.

1.2 Leveraging Our Research

The Insider Threat Center at CERT has conducted workshops and insider threat vulnerability assessments for several years. More recently, CERT has created an Insider Threat Lab to help organizations deploy technical controls. The lab's objective is to develop new controls and techniques for use with existing security tools, for example new intrusion detection system (IDS) signatures, configurations for application proxies, and behavior-based anomaly detection tools. The lab is currently testing mitigation techniques for data leakage prevention and plans to evaluate methods for dynamic modification of firewall rules. It will also test administrative controls in combination with technical and physical controls to more effectively counter insider threats; even a "silver bullet" insider threat detection tool will still require surrounding processes and policies for years to come--a fully automated solution is not likely in the near future

REFERENCES

[1] http://www.cert.org/archive/pdf/ecrimesummary10.pdf