CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Indicators and Controls for Mitigating Insider Threat

Key Message: Technical controls may be effective in helping prevent, detect, and respond to insider crimes.

Executive Summary

Insider threat continues to be one of the prime issues facing industry and government organizations worldwide. Extensive catalogues of case material from actual insider events have been used by CERT to create socio-technical models to help educate organizations on the risk of insider crime. The CERT Insider Threat team is working to demonstrate how to extract technical information from previous insider crimes to create candidate technical controls and indicators to aid in preventing, detecting, and responding to future events. [1]

In this podcast, Mike Hanley, a member of the CERT Insider Threat team, provides an update on his team’s work since the last insider threat podcast and discusses technical indicators and controls for managing insider threat, the insider threat lab, and plans for the coming year.

PART 1: DERIVING CANDIDATE INDICATORS FROM OVER 500 CASES

Insider Threat Team Update

The insider threat database now contains more than 500 actual cases of insider crimes (up from 280 since August 2009). The cases cover

- IT sabotage
- fraud
- theft of intellectual property (IP)
- espionage involving national security information

The cases come from the U.S. Secret Service and open sources such as media reports and court documents.

Additional work-in-progress includes

- system dynamics modeling of IT sabotage and two new models for theft of IP. Theft of IP addresses the question, “How can I protect my IP from a malicious insider who might steal it for financial gain?” The models address
  - entitled independence: the insider believes they own the IP due to their role in its development
  - ambitious leader: someone who recruits others to facilitate the theft of IP that they may not have direct access to
- developing models for national security espionage based on over 120 cases

Key Data for Analyzing a Case

When analyzing insider crimes, analysts are often faced with incomplete data. Some of the essential information for analyzing a crime includes

- types of assets targeted by the insider such as business plans and engineering specifications
- asset value
- insider role or type of job
- method of exfiltration such as printing a hard copy and walking out the door or sending an encrypted zip file

over a network
- intended recipient such as a competing firm
- asset value
- whether the insider has a customer in mind or is selling the information independently

A Recent Case

This case involved

- an insider in an engineering role for a firm that manufactures consumer electronics
- contact via email by a foreign competitor about a job opportunity
- a request to provide IP from the insider’s current firm as a condition of employment

This insider's actions involved

- downloading a large volume of IP within 30 days of resigning
- sending the IP via company email to the competing firm

Analysis revealed the following:

- an abnormal movement of a large volume of data on the internal network (detected using network sensors and instrumentation) from a file server that contained product specifications
- communication with a direct competitor outside of the country in violation, perhaps, of ITAR (International Traffic in Arms Regulations)
- putting these two facts together (email going to foreign competitors with large attachments) as an indicator of a potential crime

General Findings

This new work combines the Insider Threat team’s historical emphasis on behavioral indicators with new analysis on technical indicators.

For example, for theft of IP, 65 percent of insiders who steal data do so within 30 days of resigning. This is a key finding that organizations can detect and alert on.

Examples such as this can aid in developing a complete control set for testing and tuning to offer as broad guidance to interested organizations.

PART 2: PREVENT, DETECT, AND RESPOND; THE CERT INSIDER THREAT LAB

Mike’s paper Deriving Candidate Technical Controls and Indicators of Insider Attack from Socio-Technical Models and Data discusses deriving indicators and controls in three categories: prevent, detect, and respond.

Prevent

Identifying controls and indicators that might assist in preventing an insider from completing their crime is a tough problem. One example might include preventing an insider from emailing a large volume of data from a file server that stores sensitive information.

Detect

The team’s system dynamics models help identify how insiders behave when stealing information or damaging IT assets. Patterns of behavioral and technical actions provide signs or indications of malicious behavior worth investigating.

On the behavioral side, indicators can arise from the use (and violation) of

- good physical security practices
- good human resources practices
- individual managers who buy in to detecting suspicious or malicious behavior

On the technical side, indicators can arise from

- robust network instrumentation (that is already in place for normal day-to-day monitoring)
- packet capture tools
- intrusion detection systems
- firewall architectures
- host-based monitoring
- examining mail server logs for emails with large, encrypted attachments
- unexpected downloads between a client and sensitive server

Respond

Trace indicators and data left behind by insiders can aid with reconstructing what happened.

Many organizations do not prosecute insiders due to insufficient information. The most important information to capture on a regular basis is that which will help identify how the crime occurred and who committed it.

The CERT Insider Threat Lab: Demonstrating Actual Cases

The insider threat team is developing the capability to demonstrate actual cases in scenarios that can be used to teach people how to identify patterns and indicators associated with insider crimes.

Scenarios include both behavioral and technical patterns and the use of tools, for example

- alerting on email sent to a competitor domain name
- examining time stamps that show emails with large attachments being sent seven days before the insider is scheduled to leave the organization
- using tools such as Splunk (a centralized log aggregator) for organization-specific search queries on indicators of interest

Such demonstrations aid those working in security and network operations centers who are concerned about insider threat.

PART 3: KEY ROLES FOR USING INDICATORS; FUTURE RESEARCH DIRECTIONS

Target Audience

The primary audience for this work is those working in security operation centers such as technical staff who are monitoring key sensors (firewall logs, log aggregators, intrusion detection systems) for system and network performance.

System and network administrators are able to use many of the same tools for monitoring what’s coming in from the outside world to aid in detecting what’s going on inside.

Upcoming Plans

Near-term plans include

- as part of the Insider Threat Lab, investigating tools and techniques for detection and response including the repurposing of existing network security tools to inform promising indicators
- doing more work at the intersection of the behavioral and technical spaces
- defining and documenting a good set of standard controls with justification
- testing indicators and controls with pilot organizations
- developing guidance for customization

It is important to keep in mind that these are *candidate* controls and indicators. Many cases go unreported and many cases are undetected. So the CERT Program's work is only based on reported cases of those who got caught.

Resources

[1] Hanley, Michael. "Deriving Candidate Technical Controls and Indicators of Insider Attack from Socio-Technical Models and Data". *Proceedings of the 2010 CAE Workshop on Insider Threat*, November 2010.

The CERT Insider Threat website

CERT Podcasts on Insider Threat

- Mitigating Insider Threat: New and Improved Practices (August 2009)
- Insider Threat and the Software Development Life Cycle (March 2008)
- Protecting Against Insider Threat (November 2006)