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

Mitigating Insider Threat: New and Improved Practices

Key Message Preventing and detecting insider threat is greatly improved by implementing 16 best practices based on 282 cases.

Executive Summary

The purpose of CERT's insider threat research "is to maintain a current state of awareness of the methods being used by insiders to commit their attacks as well as new organizational issues influencing them to attack. New and updated practices (build upon past work and) are based on analyzing approximately 100 recent insider threat cases that occurred from 2003 to 2007 in the U.S." [Cappelli 09] Recent theft and fraud cases highlight theft and modification of information for financial gain and business advantage.

In this podcast, Dawn Cappelli, Andy Moore, and Randy Trzeciak, members of CERT's Threat and Incident Management Team, discuss 7 of their latest best practices for preventing and detecting insider threat. This work serves as the basis for a new insider threat workshop and risk assessment.

PART 1: ANALYZING REAL-LIFE CASES; ASSESSING RISK & RAISING AWARENESS

Defining Malicious Insider

A malicious insider is "a current or former employee, contractor, or business partner who has or had authorized access to your network, your systems, your data, and intentionally misused that access." Due to recent trends business partners have been added to the definition.

This definition does not include accidental data leakage or espionage involving national security information.

Cases Analyzed to Date

CERT's insider threat database currently holds 282 cases, from 1996 to the present. They comprise four categories:

- Sabotage: an insider wants to cause harm to the organization or to a person, for example, wiping out data, bringing down systems, and disrupting operations. There are currently 101 sabotage cases.
- Theft of intellectual property: an insider steals trade secrets, business plans, strategic plan, or any type of intellectual property. There are currently 40 intellectual property cases.
- Theft or modification for financial gain: an insider steals personally identifiable information, credit card information, or other types of information that can be sold. This also includes modifying information in, for example, a database for financial gain. There are currently 106 cases of this type.
- Miscellaneous: There are 41 cases that do not clearly fall into one of the above categories or they may span categories.

Practice 1: Insider Threat & Risk Assessment

This practice states: Consider threats from insiders and business partners in enterprise-wide risk assessments.

Organizations often fail to recognize that they need to pay attention to those outside of their organization such a business partners, consultants, contractors, and those with whom they collaborate, partner, or associate.

Such parties often have full access to your critical data, processes, information, and information systems. So they need

to be considered when assessing risk.

A Recent Case

A consumer data organization was responsible for accepting data from banks, phone companies, and credit card companies. They would analyze this data and provide marketing information in return.

The consumer data organization subcontracted with a data mining company. A system administrator with the data mining company ran a password cracker to obtain passwords for all customer databases managed by the consumer data organization. He downloaded millions of records and solicited them for sale on the Internet.

This illustrates what can happen when sensitive data is outside the control of the owning organization.

Such incidents can be somewhat mitigated by ensuring proper security requirements are written into contracting agreements that are comparable to those used by the owning organization. This includes requiring that contractors and subcontracts notify you immediately when authorized users leave their organizations so you can disable their access, both electronic and physical.

This is a critical issue when working with cloud service providers.

Practice 3: Security Awareness

This practice states: Institute periodic security awareness training for all employees.

Unique aspects of insider threat security awareness include these myth busters:

- The age of insiders is from late teens to retirement.
- Insiders include both men and women.
- Insiders are stereotypical introverted loners as well as aggressive individuals, high performers, and extroverted star players.

As a result, insiders are best identified by their behavior, not stereotypical characteristics or profiles. Such behaviors include insiders that:

- make threats against the organization
- brag about the damage they could do
- demonstrate excessive or uncharacteristic interest in information outside of their domain

Managers need to be aware of these behaviors, monitor for them, document them, and communicate them to key stakeholders such as Human Resources. Such communication is critical for determining when to take action.

It is particularly important to watch for these behaviors in advance of resignation or termination.

PART 2: LEAST PRIVILEGE & SEPARATION OF DUTIES; PASSWORD & ACCOUNT MANAGEMENT

Practice 8: Enforce Least Privilege & Separation of Duties

Least Privilege

Insiders tend to steal what they have authorized access to. And they often have access to more than they need. Least privilege enforces limited access.

In one case, a salesman was able to steal source code for a new product, yet someone in this role does not require access to source code.

Least privilege is difficult to maintain as roles and responsibilities change frequently. But managers should keep a good handle on who has access to what.

Separation of Duties

This principle typically requires that two or more people are involved in taking some action: one to perform it and one to approve it. Even if this practice is in place, it is often not enforced by technology controls.

Given their broad privileges, system administrators in particular should be subject to stringent separation of duties controls.

In one case, a system administrator was demoted from senior to junior status (only able to access a single server) but this change was not enforced. He was able to plant a logic bomb on multiple servers, modify system logs, and frame his supervisor for the bad acts.

Most account management sabotage cases occur after the insider leaves the organization. Prior to departure, they create unknown access paths back into the system using shared accounts or backdoor accounts that appear legitimate.

Practice 7: Password Management

This practice states: Implement strict password and account management policies and practices.

Users will often share passwords to get around separation of duties. Weak passwords are also easily cracked and then used to create unknown access paths.

Organizations need to pay attention to current and former employees when it comes to effectively and correctly managing accounts, and enforcing least privilege and separation of duties.

Practice 10: Privileged Users

This practice states: Use extra caution with system administrators and technical or privileged users.

The majority of insiders who committed sabotage held some type of technical position. More than half of these stole confidential or proprietary information.

Separation of duties (also known as two person rule) is often subverted by:

- writing or downloading scripts or programs
- installing logic bombs that go off after insiders leave the organization
- creating back door accounts
- installing system administration tools that support remote access
- modifying system logs to delete malicious actions and frame others
- installing malicious code

In one case, a system administrator left his position without advance notice. The organization withheld pay. Due to no enforcement of separation of duties, the system administrator was able to:

- change administrator passwords until he was paid
- access email
- modify systems to prevent single user access
- access and modify key system files

Two-person rule can be used to ensure that changes to critical systems, files, and data involve at least two parties.

PART 3: LOGGING, MONITORING, & AUDITING; INCIDENT RESPONSE

Practice 12: Logging, Monitoring, & Auditing

This practice states: Log, monitor, and audit employee actions online.

Users can be held accountable for their actions through logging, monitoring, and auditing. The creation and use of backdoor accounts, installation of downloaded software, and testing of malicious code can be detected using these tools.

Most intellectual property theft occurs within one month of resignation and involves very large downloads of information outside of the insider's domain of responsibility.

In one case, a chemist accessed 116,000 pdf files and downloaded 22,000 abstracts in the four months prior to and after his resignation. This information came from the server that contains many of the organization's trade secrets.

The key concepts here are a known window of opportunity with a known signature or pattern that can be detected by logging, monitoring, and auditing.

Practice 16: Incident Response

This practice states: Develop an insider incident response plan.

Many organizations have a common misperception – that insider threat can be solved solely by information security, information technology, and technical controls.

This is not the case. In addition to information security and IT departments, others need to be involved including:

- human resources
- legal
- managers
- physical security
- data owners
- law enforcement

Communication among these groups is essential. Observing and communicating high-risk behaviors that fit these profiles and patterns in the timeframes where they typically occur can aid in mitigation.

According to the 2007 E-Crime Watch Survey, 70 per cent of organizations experiencing an insider electronic crime handled the crime internally without legal action or involving law enforcement.

Law enforcement can provide essential resources to investigate and prosecute crimes.

Insider Threat Risk Assessment

CERT provides a 3-day insider risk assessment that covers all of the issues of concern raised in the cases analyzed to date, along with suggested countermeasures. One of the benefits is to get all of the stakeholders described above together so they can each understand their own and one another's roles.

Attendees are better able to determine what situations are most relevant for their organizations and then identify and prioritize risks as part of their larger risk management strategy.

Insider Threat Workshop

Building upon seven-and-a-half years of research, this two-day workshop consists of presentations and interactive

exercises. Participants take away actionable steps to better manage the risk of insider threat in their organizations.

Resources

CERT's Insider Threat website

[Cappelli 09] Cappelli, Dawn; Moore, Andrews; Trzeciak, Randall; Shimeall, Timothy. "Common Sense Guide to Prevention and Detection of Insider Threats 3rd Edition – Version 3.1." Carnegie Mellon University, Software Engineering Institute, CERT Program, January 2009.