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

Mitigating Insider Threat: New and Improved Practices Fourth Edition

Key Message: 371 cases of insider attacks lead to 4 new and 15 updated best practices for mitigating insider threat.

Executive Summary

"The fourth edition of the *Common Sense Guide to Mitigating Insider Threats* introduces the topic of insider threats, explains its intended audience and how this guide differs from previous editions, defines insider threats, and outlines current patterns and trends. The guide describes 19 practices that organizations should implement across the enterprise to prevent and detect insider threats, as well as case studies of organizations that failed to do so. Each practice includes features new to this edition: challenges to implementation, quick wins and high-impact solutions for small and large organizations, and relevant security standards. The appendices provide a revised list of information security best practices, a new mapping of the guide's practices to established security standards, a new breakdown of the practices by organizational group, and new checklists of activities for each practice." [1]

In this podcast, George Silowash and Lori Flynn, members of CERT's Insider Threat Center, summarize what has changed since the third edition, published in January 2009. They discuss the four new practices that are described in the guide, including relevant cases and quick wins.

PART 1: OVER 370 CASES ANALYZED TO IDENTIFY PRACTICES

Definition of an Insider

An insider is a current or former employee, contractor, or business partner who:

- has or had authorized access to an organization's network, system, or data
- has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems

Cases, Categories, and Sectors

More than 700 cases of insider attacks have been analyzed to date, categorized as follows:

- intellectual property (IP) theft
- fraud
- IT sabotage
- espionage
- miscellaneous

The top six infrastructure sectors affected by these attacks include:

- banking and finance
- IT
- healthcare and public health
- federal government
- state and local government
- commercial facilities

For this edition of the Common Sense Guide (CSG), 371 cases were analyzed (espionage was excluded). All 371 cases

have been adjudicated – the insider was found guilty in a court of law.

Sources for cases include:

- media
- law enforcement organizations (such as the FBI and the U.S. Secret Service)
- organizations with whom CERT has trusted relationships

CERT has teamed with the U.S. Secret Service to develop an annual survey about insider threat (called the CyberSecurity Watch Survey). According to the latest survey, 76 percent of insider threat cases are not reported to law enforcement or the media.

PART 2: WHAT'S NEW IN V4; CLOUD SERVICE AGREEMENTS

Improvements from the Third Edition (January 2009)

New and improved content reflected in the fourth edition of the CSG include:

- more cases
- 4 new practices; 15 updated practices (folded the v3 software development practice into others)
- one or more case examples with each practice, where possible
- guidance for a range of roles: human resources, legal, physical security, data owners, information technology, information assurance and software engineering
- quick wins and high-impact solutions for each practice—a list of suggested quick wins per practice for jump-starting an organization's insider threat program. These are tailored to large and small organizations.
- mapping to selected standards including NIST 800-53, ISO 27002, and CERT-RMM.

Quick wins apply to large and small organizations and can help build momentum for adding new practices and improved processes.

New Practice: Cloud Service Agreements

The full practice 9 statement is "Define explicit security requirements for any cloud services, especially access restrictions and monitoring capabilities." The motivation for this new practice is the growth in the use of cloud computing – to consolidate systems and save money.

Organizations considering using cloud services need to:

- assess the provider's physical and logical security and access controls
- ensure controls will protect the confidentiality, integrity, and availability of data at rest, data in motion, and data in use
- understand who has access to data and infrastructure, within their organization and within the cloud provider's organization
- assess risks and mitigate them to an acceptable level

Case Example

A retail organization used two-factor authentication tokens for remote access. A network engineer was fired. The insider:

- before departing, created a token in the name of a fake employee
- one month after termination, contacted the IT department using a fictional name and convinced them to activate the token
- several months later, used the VPN token to access the network, delete virtual machines, shut down the storage area network, and delete email accounts

It took the IT staff more than 24 hours to restore operations, costing more than $200,000.

Quick Win

Verify the cloud provider's hiring practices and ensure that they conduct thorough background security investigations on all personnel (operations staff, technical staff, and even janitorial staff). This should be done prior to hiring and on a periodic basis.

Some cloud providers do tailor their services to regulated sectors including the U.S. federal government. They understand the need for more rigorous controls and are willing to be more transparent.

PART 3: NETWORK BEHAVIOR; SOCIAL MEDIA

New Practice: Network Behavior

The full practice 17 statement is "Establish a baseline of normal network device behavior."

To differentiate normal from anomalous behavior, organizations need to capture baseline data that can be monitored and analyzed for security events and unusual behavior at the enterprise, department, group, and individual user level including:

- network topology
- bandwidth utilization
- usage patterns
- protocols
- ports
- internal and external connection counts
- byte counts for email attachments
- device sets that work stations and servers communicate with
- firewall and IDS (intrusion detection system) alerts

Analyze these to see what is normal, what is a variation, and what is unusual.

Once a baseline is established, deviations from normal behavior can signal possible security incidents, including those perpetrated by insiders.

Case Example

Four months prior to departing, an insider, responsible for research and development projects:

- downloaded a high volume of trade secrets (17,000 PDFs and 22,000 abstracts)
- did so on site, during working hours, over a few 15-20 hour periods of time

This activity was 15 times greater than that of the next highest user and the data was not related to his research. So this behavior could have been detected through monitoring, which would have triggered an alert based on a significant departure from normal behavior.

This activity was not detected until the insider resigned. The stolen intellectual property was valued at $400,000,000.

Quick Win

Use network monitoring tools to monitor the network for a period of time and establish a baseline of normal behavior and trends.

Approaches include:

- trigger an alert for anomalous, high activity that occurs after normal working hours
- start small first (for example, data downloads and data accesses), then add more
- use commercial and open source tools

New Practice: Social Media

The full practice 18 statement is "Be especially vigilant regarding social media."

Today, many people seem to want to share everything about themselves and their life. Organizations need to be aware of the risks that this may pose based on the behavior of their users.

Information posted to a social media site could be used to conduct a social engineering campaign against the organization and its employees, resulting in financial and other losses.

The best way to mitigate this risk is through training.

Case Example

An attacker compromised the email account of a former U.S. vice presidential candidate as follows:

- used a search engine to find the answers to password recovery questions (date of birth, zip code, where she met her spouse)
- used this information to reset passwords on an email account
- accessed her email and posted it to a public form

Quick Win

Include social media training as part of the organizations' annual security awareness training program.

PART 4: DATA EXFILTRATION

New Practice: Data Exfiltration

The full practice statement is "Close the doors to unauthorized data exfiltration."

Data exfiltration means that the data moves to an unauthorized location. This can happen electronically or physically.

To address this risk, an organization needs to:

- identify its critical assets (information, technology, facilities), selecting those that are at the highest risk
- identify users who have authorized access to these assets
- determine asset physical locations, including all devices that connect both physically and wirelessly

Examples of devices that could be used to exfiltrate data include:

- smartphones
- thumb drives
- printers
- scanners
- fax machines
- mp3 players
- microphones
- video conferencing systems

- internet services such as instant messaging, SSH (secure shell), FTP (file transfer protocol), and email

To mitigate this risk, an organization needs to implement relevant policies (for example, BYOD (Bring Your Own Device)), technical and physical controls, and compliance reviews. The challenge is to balance security controls that help prevent exfiltration with user productivity.

Challenges

Data is scattered everywhere, across the organization. Understanding where the data is and its sensitivity can be a significant undertaking. CERT has published several technical reports that describe various aspects of this issue and how to address it (see Resources).

Case Example

While at a customer site, a tax preparation service employee printed personally identifiable information on at least 30 customers. The insider later used the Social Security numbers to submit fraudulent tax returns, receiving refunds totaling $290,000.

Quick Win

Restrict data transfer protocols, such as FTP or SCP (session control protocol), to employees with a justifiable business need and carefully monitor their use. These protocols can export a high volume of data very quickly.

Resources

CERT Insider Threat website

[Silowash 2012] Silowash, George, et al. *Common Sense Guide to Mitigating Insider Threat, Fourth Edition* (CMU/SEI-2012-TR-012). Software Engineering Institute, Carnegie Mellon University, December 2012.

Silowash 2013] Silowash, George & King, Christopher. *Insider Threat Control: Understanding Data Loss Prevention (DLP) and Detection by Correlating Events from Multiple Sources* (CMU/SEI-2013-TN-002). Software Engineering Institute, Carnegie Mellon University, January 2013.

[Silowash 2013] Silowash, George & Lewellen, Todd. *Insider Threat Control: Using Universal Serial Bus (USB) Device Auditing to Detect Possible Data Exfiltration by Malicious Insiders* (CMU/SEI-2013-TN-003). Software Engineering Institute, Carnegie Mellon University, January 2013.

[Hanley 2011] Hanley, Michael & Montelibano, Joji. *Insider Threat Control/Using Centralized Logging to Detect Data Exfiltration Near Insider Termination* (CMU/SEI-2011-TN-024). Software Engineering Institute, Carnegie Mellon University, October 2011.