CERT PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Protecting Against Insider Threat

Key Message: The threat of attack from insiders is real and substantial. Insiders have a significant advantage over others who might want to harm an organization.

Executive Summary

Over the past several years, CERT has been conducting a range of research projects on insider threat. One of the conclusions reached is that insider attacks have occurred across all organizational sectors, often causing significant damage to the affected organizations. These acts have ranged from "low-tech" attacks, such as fraud or theft of proprietary information, to technically sophisticated crimes that sabotage the organization's data, systems, or network. Damages are not only financial. Widespread public reporting of the event can also severely damage the organization's reputation.

In this podcast, Dawn Cappelli, leader of CERT's research efforts on insider threat, discusses the issues and why leaders need to take action. The actions are not always those you might suspect.

PART 1: THE THREAT

Background

CERT has been studying insider threat since 2002, starting with an insider threat study conducted with the United States Secret Service. This study involved analysis of 150 insider threat cases.

Insider-threat crimes (deliberate, malicious activity) fall into three categories:

- fraud
- theft of confidential information
- IT sabotage

CERT has conducted an electronic crime survey for the past three years with the U.S. Secret Service and CSO Magazine. Last year, 20% of all electronic crimes were reportedly committed by insiders. This year, it was 27%. Last year, 39% of organizations surveyed experienced as least one insider incident. This year, that percentage increased to 55%. Leaders need to pay attention, given that insider threat appears to be on the rise.

The Trust Trap

It is critical to be diligent in monitoring the behavior of current employees and to view insider threat as much more than a technical issue. It is important to understand the big picture, including the

- psychology of insiders
- impact of the organizational culture on insider behavior
- impact of policies, procedures, practices, and technology

Interview with a Convicted Insider

One convicted insider was the top foreign currency trader working for an investment firm. Over a period of five years, he stole $691 million and had kept this hidden.

How could this happen?

He was the star performer, so he was above suspicion and became irate when questioned. He intimidated management into ignoring the signs of his crime.

He was both the trader and the programmer of the software he used to commit the crime. This indicates an absence of: separation of duties, integrity checking, and independent checks and balances.

PART 2: WARNING SIGNS

All sectors are at risk, although fraud is most often a financial sector issue. Information can be stolen by financially motivated or disgruntled employees (or former employees) in any organization in any sector, using something as commonplace as Social Security numbers.

Theft of Confidential Information

Those stealing proprietary information were often leaving to go to a new job. For example, sometimes they didn't even realize that taking software they had developed was illegal if their new employer was not a competitor of their former employer.

Sometimes the new employer turned the new employee in to their former employer!

Disgruntled employees offered to sell information to a competitor. And, again, often the competitor would turn them in.

IT Sabotage

Committed by system administrators and database administrators; the most technical form of insider crime.

These crimes have very distinct patterns:

- The insider has a personal predisposition to commit the crime. They are unable to handle conflict or disappointment in the same way that other people do.
- Over 30% have an arrest history that should have been picked up in a background check.
- They exhibit "concerning behaviors" such as getting angry or upset with modest provocation, and holding a grudge. They yell at people, perform poorly, or are late for work.

Often, these behavioral precursors are ignored, and then things escalate. If management is paying attention, they can catch these situations before they become more serious.

Typically, behavioral precursors are followed by technical precursors. The following technical precursors can be detected by increased technical monitoring:

- Creating backdoors
- Downloading password crackers and running them on employee accounts
- Creating logic bombs set to go off at some future time

Impact of Sanctions

Fifty-seven percent of insiders who committed IT sabotage were former employees, so they committed attacks after they left.

Many could see their termination coming, so they created backdoor accounts that they could use to launch an attack at some future time. These are called "unknown access paths."

PART 3: MITIGATING INSIDER THREAT

Security Awareness Training

- Make sure employees who notice something suspicious know who to contact and when they should do so.
- Passwords should not be shared, even if doing so would make teamwork easier.
- Separation of duties is critical to enact required checks and balances.

By sharing passwords, users risk their accounts being used to commit an illegal act. System logs reveal all. Technically sophisticated insiders know this, and they are able to conceal their actions and shift blame to an innocent party.

Protect System Logs so they can't be modified, such as by using "append only" controls.

Account Management

In addition to setting up accounts with appropriate and least privilege access, organizations need to ensure that

- accounts are monitored and reviewed to ensure they are legitimate. In one case, a former employee set up VPN (virtual private network) accounts for legitimate employees that they didn't know about, and then used these after he left.
- account management policy is enforced.
- accounts and permissions are updated, particularly when people leave or when roles change.

Use Characterization Processes to establish trusted, baseline software configurations. These configurations can then be compared to current production configurations to detect malicious and rogue software.

Conduct Enterprise-Wide Risk Assessments to determine which critical assets require the highest levels of protection, given that you can't protect everything.

Next Steps

- Become better informed about the problem.
- Realize that insider threat is both a people problem and a technical problem.
- Understand behavioral and technical precursors.
- Implement recommended practices.

Resources

Cappelli, Dawn; Moore, Andrew; Shimeall, Timothy. Common Sense Guide to Prevention and Detection of Insider Threats. Carnegie Mellon University CyLab, April 2005.

2006 E-Crime Watch Survey (pdf)

CERT Insider Threat website

Rasmussen, Gideon. Insider Risk Management Guide. SearchSecurity.com, 30 August 2006.

Rasmussen, Gideon. Insider Threat website.