Carnegie Mellon
Software Engineering Institute
CERT® Coordination Center

U.S Department of Homeland Security

United States Secret Service

Press Release

May 16, 2005
Secret Service Contact: (202) 406-5708
CERT Contact: (412) 268-4793
PUB 11-05

SECRET SERVICE AND CERT RELEASE REPORT ANALYZING ACTS OF INSIDER SABOTAGE VIA COMPUTER SYSTEMS IN CRITICAL INFRASTRUCTURE SECTORS

Second in a Series of Reports Focusing on Insider Threats to Information Systems and Data in Critical Infrastructure Sectors

(Washington, DC) — The United States Secret Service and the Carnegie Mellon Software Engineering Institute's CERT today announced the findings of the second Insider Threat Study report. According to the report, which analyzed acts of insider sabotage on computer systems in critical infrastructure sectors, the majority of insiders who committed the attacks were former employees, motivated at least in part by a desire to seek revenge and who were granted system administrator or privileged access when hired.

The goal of the Insider Threat Study, made possible in part by financial support from the U.S. Department of Homeland Security's Science and Technology Directorate, is to better understand malicious insider activities affecting information systems and data in critical infrastructure sectors. The study is the first of its kind to provide a comprehensive analysis of insider actions by analyzing both the behavioral and technical aspects of the threats.

"At a time when homeland security is more closely linked than ever to the protection of our nation's critical infrastructure, the Insider Threat Study serves as an important reminder for all of us to protect sensitive information by closely monitoring and safeguarding network usage and reporting suspected intrusions to security personnel and law enforcement as soon as a breach is detected," said United States Secret Service Director Ralph Basham.

The Findings

Forty-nine cases, carried out between 1996 and 2002, were examined across critical infrastructure sectors. These cases were purposely limited to those in which an insider's primary goal was to sabotage some aspect of the organization or direct specific harm toward an individual.

The study revealed:

- A negative work-related event triggered most of the insiders' actions.
- Sixty-two percent of incidents were planned in advance.
- Eighty percent of the insiders exhibited unusual behavior in the workplace prior to carrying out their activities.
- Fifty-seven percent of insiders exploited systemic vulnerabilities in applications, processes and/or procedures.
- Thirty-nine percent used relatively sophisticated attack tools.
- Sixty percent of insiders compromised computer accounts, created unauthorized backdoor accounts or used shared accounts in their attacks.
- Most incidents were carried out via remote access.
- Less than half of the insiders (43%) had authorized access at the time of the incident.
- Insider activities caused financial losses (81%), negative impacts to business operations (75%) and damage to the organizations' reputations (28%).

"The power of a terminated employee with system administrator access should not be underestimated," said Dawn Cappelli, senior member of the technical staff with CERT. "Some organizations completely neglect disabling access upon termination. Others go through the steps to disable access, but the insider is able to find that one access control gap that was overlooked. It is important that technical staff are attentive to the obscure methods used in the insider attacks in this study."

Implications

This report suggests important proactive strategies by all levels of an organization's personnel to mitigate insider threats. These strategies include detailed suggestions for best practices for information security and human resources that historically have not been consistently implemented. Specifically, the report suggests:

- Disabling access following termination
- Management attention to negative events in the workplace
- Establishing formal grievance procedures as an outlet for insider complaints
- Creating reporting processes for when a colleague notices or suspects concerning behavior
- Enforcing comprehensive password policies, computer account management practices and layered security for remote access
- Using configuration management practices for detection of logic bombs and malicious code
- System logging and monitoring, and backup and recovery procedures

About the Insider Threat Study
The Insider Threat Study is a collaborative research endeavor between the Secret Service's National Threat Assessment Center (NTAC) and CERT, designed to develop information to help private industry, government and law enforcement better understand, detect, and ultimately prevent harmful insider activity. The definition of an insider for this study includes current, former, or contract employees of an organization.

Previously, in August 2004, the first report of the Insider Threat Study was released*: Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector.* It focused on the people who had access to and perpetrated harm using information systems in the banking and finance sector, which includes credit unions, credit bureaus and other financial institutions.

About the Secret Service's National Threat Assessment Center
The Secret Service has taken a lead role in the developing area of cyber crime, establishing working partnerships in both the law enforcement and business communities to address such issues as protection of critical infrastructure, internet intrusions and associated fraud.

The National Threat Assessment Center was created by the Secret Service in 2000 to provide leadership and guidance to the emerging field of threat assessment. Two previous NTAC studies, the Exceptional Case Study Project and the Safe School Initiative, analyzed physical attacks on public officials and public figures and attacks on schools. Both studies focused on identifying information that was operationally relevant and that could help prevent future violent or disruptive incidents. Findings from the Insider Threat Study may similarly enhance efforts within law enforcement, corporate security, information technology, and others in prevention, early detection, and investigation of cyber-related crimes.

About CERT
CERT is located at Carnegie Mellon University's Software Engineering Institute (SEI) in Pittsburgh, Pennsylvania, USA. The SEI is a U.S. Department of Defense sponsored federally funded research and development center. The CERT Coordination Center, an initiative within CERT, was established in 1988 to deal with security issues on the Internet. It also partners with and supports the U.S. Department of Homeland Security's National Cyber Security Division and its US-CERT to coordinate response to security compromises, identify trends in intruder activity, identify solutions to security problems, and disseminate information to the broader community. CERT also conducts research and development to create solutions to security problems and provides training to help individuals build skills in dealing with cyber-security issues.

###

EDITOR'S NOTE: The complete report from the Insider Threat Study can be found at http://www.secretservice.gov/ntac.shtml and http://www.cert.org/archive/pdf/insidercross051105.pdf

For questions concerning this release, please contact the United States Secret Service Office of Government and Public Affairs at 202-406-5708 or Kelly Kimberland at CERT® at 412-268-4793.