http://www.sei.cmu.edu/newsitems/insider-book.cfm

New Insider Threat Guide Draws on Ten Years of SEI Research

A night-shift security guard at a hospital plants malware on the hospital's computers. The malware could have brought down the heating, ventilation, and cooling systems and ultimately cost lives. Fortunately, he has posted a video of his crime on YouTube and is caught before carrying out his illicit intent.

A programmer quits his job at a nuclear power plant in the United States and returns to his home country of Iran with simulation software containing schematics and other engineering information for the power plant.

A group of employees at a Department of Motor Vehicles work together to make some extra money by creating driver's licenses for undocumented immigrants and others who could not legally get a license. They are finally arrested after creating a license for an undercover agent who claimed to be on the "No Fly List."

The impact of insider attacks has been devastating: trade secrets worth hundreds of millions of dollars have been lost to foreign countries or competitors, competing products based on stolen information have been brought to market by former employees and contractors, funds have been stolen outright, and corporate reputations have been irrevocably damaged. Since 2001, a team of researchers in the SEI's CERT® Program has been studying the problem of cybercrimes committed by current or former employees, contractors, or business partners of the victim organization. During that period, the CERT Insider Threat Center assembled a detailed archive of more than 700 cases like the ones highlighted summarized above. This database has formed the foundation for the CERT Insider Threat Center's research, work that has produced numerous reports detailing the problem and identifying mitigation strategies, administrative and technical controls for combatting the insider threats, system dynamic models that characterize the nature of the risk and inform detection and response strategies, and an assessment framework to help organizations identify areas of exposure.

The work of the CERT Insider Threat Center has also resulted in The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). Published by Addison-Wesley Professional, this book digests ten years of CERT research on the problem of insider threat into a practical guide. It offers specific guidance and countermeasures that can be immediately applied by executives, managers, security officers, and operational staff within any private, government, or military organization.

“This book provides a comprehensive reference for our entire body of knowledge on insider threats,” said Dawn M. Cappelli, Technical Manager of CERT’s Enterprise Threat and Vulnerability Management Team, which includes the CERT Insider Threat Center. “We use many case examples from the CERT database throughout. We believe these real-world examples will open the reader’s eyes to the many facets of the problem and get them asking relevant questions about their own organization’s exposure.”

In The CERT Guide to Insider Threats, Cappelli and her coauthors Andrew P. Moore, CERT Insider Threat Center lead researcher, and Randall F. Trzeciak, Technical Lead of Insider Threat Research systematically address attacks by various types of malicious insiders, including current and former employees, contractors, business partners, outsourcers, and even cloud-computing vendors. They also analyze the three major types of insider cybercrime: IT sabotage, intellectual property theft, and fraud. For each, they present a crime profile, describe how the crimes evolve over time, and detail the motivations, attack methods, organizational issues, and precursor warnings that could have helped the organization prevent the incident or detect it earlier. Beyond identifying crucial patterns of suspicious behavior, the authors present concrete defensive measures for protecting both systems and data.

The book also conveys the big picture of the insider threat problem over time: the complex interactions and unintended consequences of existing policies, practices, technology, insider mindsets, and organizational culture. Most importantly, it offers actionable recommendations for the entire organization, from executive management and board members, to information technology staff, data owners, human resources representatives, and legal departments.

“We use many case examples from the CERT database throughout. We believe these real-world examples will open the reader’s eyes to the many facets of the problem and get them asking relevant questions about their own organization’s exposure.” – Dawn M. Cappelli, Technical Manager of CERT’s Enterprise Threat and Vulnerability Management Team

“From the beginning, we tried to focus on describing the problem as more than a strictly technical challenge,” said Trzeciak. “This problem cannot be solved by technical measures alone, and it involves the entire enterprise. Yes, information technology is a core component, but there are non-technical aspects organizations need to consider. The entire organization has a stake in this problem.”

Moore explained that the authors had this wide audience in mind when writing The CERT Guide to Insider Threats. “Because the problem affects so many organizational departments,” said Moore, “we took pains to present the information, including technical solutions, in a way that a general audience can understand.” Moore explained that only one section of the book—the section focused on technical controls—is intended for a purely technical audience.

As with other security challenges facing CERT, the problem of insider threat continues to evolve and the CERT Insider Threat Center has begun to focus on emerging threats and challenges. “We’re moving on three key areas in the coming year,” said Cappelli. “First, we’re focusing

"This problem cannot be solved by technical measures alone, and it involves the entire enterprise. Yes, information technology is a core component, but there are non-technical aspects organizations need to consider."– Randall F. Trzeciak, Technical Lead of Insider Threat Research

efforts in our Insider Threat Lab on development of new technical controls. Specifically, we're examining how organizations can take advantage of their investment in existing technologies and use them to detect insider threat. Second, we're working on strategies and resources that can help organizations in government and industry stand up formal insider threat programs." Cappelli explained that the focus in the community to date has been mostly informal and highly reliant on technical solutions. However, in light of recent high-profile insider threat incidents, such as Wikileaks, the U.S. government has begun to realize the need to establish a formal insider threat program.

Third, the team has the problem of unintentional insider threat on its radar. "External intrusions are often facilitated by insiders inadvertently exposing their organization to attack," said Moore. "External attackers realize that insider error—such as falling for a spear fishing or similar attack—is an important tool they can exploit."

But the proven insider attack methods aren't going away. "We've found over the last 10 years that the information we've assembled in The CERT Guide to Insider Threats still holds," said Cappelli. "That's why we believe this book will stand the test of time and provide a useful resource for years to come."

For more information about the CERT Program's research on insider threat, please visit http://www.cert.org/insider_threat/.

For more information about The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud), and to read a chapter, please visit http://www.informit.com/store/product.aspx?isbn=9780321812575.