Military Information Technology
The Voice of Military Communications and Computing

Login
Tuesday, 12 Ja

Search...

- HOME
- ADVERTISE
- SUBSCRIBE
- EVENTS
- ARCHIVES
- CONTACT US

CURRENT ISSUE

***Issue 13, Volume 11 December 2009***

**KMI MEDIA GROUP WEBSITES**

**SUBSCRIPTION SERVICES**

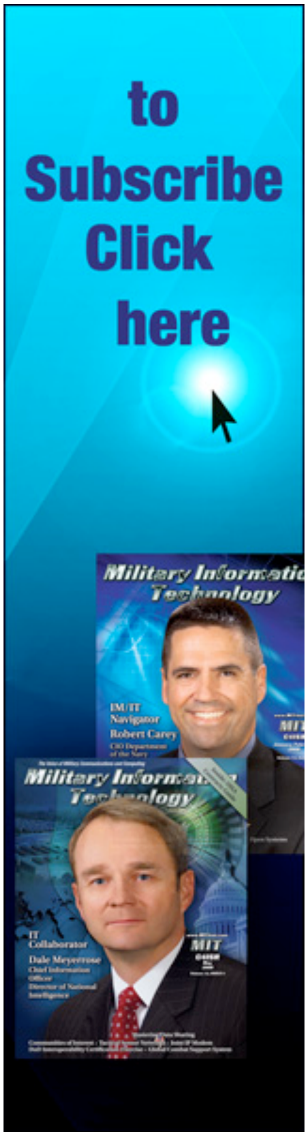
# Insider Threats: The Devil You Know

Written by Karen D. Schwarz

MIT 2009 Volume: 13 Issue: 10

SUGGESTION BOX

# Varied Technologies Help Defense Agencies Take Proactive Approach to Counter Potential Network Security Risks Posed by Employees and Contractors.


to
Subscribe
Click
here
Military Information Technology
IM/IT Navigator Robert Carey
Military Information Technology
IT Collaborator Dale Meyerrose

As they strive to prevent security breaches caused by those with legitimate access to networks, military agencies are turning to a variety of technologies designed to counter the "insider threat."

More than ever before, all organizations must bolster their forces against insiders who either intend to do them harm or do so unwittingly. The threat is growing exponentially, with one estimate finding that more than half of all serious data breach incidents are caused by employees, contractors and similar personnel.

All insider threats aren't created equal, but they can be equally harmful. One type is outright sabotage, where the insider wants to cause harm to the organization or to a person. A second is theft of intellectual property, which involves insiders stealing important institutional data such as strategic plans. A third category involves modifying sensitive information for financial gain. The fourth type is unintentional, either by doing something unknowingly harmful or by being used as a pawn by another insider or outside hacker.

By far, most insider threats are intentional. According to Carnegie Mellon University's CERT program, the methods used by insiders are varied, including downloading of scripts or programs, deploying logic bombs prior to leaving the organization, creating backdoor accounts, installing remote administration tools or embedding malicious code.

When it comes to the military, the threats and the stakes are higher. If a mission-critical system is brought to its knees, lives may hang in the balance. And if information related to national security is compromised, the costs can be catastrophic, noted Aaron Higbee, chief technology officer of Intrepidus, a security provider. What is also different about the military is the lengths to which adversaries will go. Attackers—even internal attackers—who aspire to compromise the military's systems tend to be well-trained, use sophisticated techniques, and go to great lengths to hide their tracks.

## CONTRACTORS AND COLLABORATION

Complicating this scenario is the military's reliance on external contractors, both domestic and from around the world. "The Department of Defense relies on corporations providing weapons systems and other outsourced services, which expands its perimeter and makes the organization large and vulnerable," said Jon Ramsey, chief technology officer for SecureWorks, an information security vendor. "Insiders can become part of the organization by working for a company that provides that technology. They do get vetted, but the military has become so dependent on third-party companies that if you wanted to get secrets for the military, you would probably work for a company that already has a relationship with the military, and so might have a less rigorous vetting process."

The current focus on collaboration makes security an even tougher challenge.

"When I worked for the government and was stationed overseas 13 years ago, a lot of the projects were isolated from one another, so there wasn't a lot of concern that somebody who happened to have an account on your network could reach across the network into other projects or classified areas," said Eddie Schwartz, now chief security officer of NetWitness, a provider of security solutions for government.

"But today, because of all of the interconnectivity and a greater desire in the military and intelligence community to share data, a person working inside of the network can potentially reach out to a lot more data stores and resources than they could in the past. If you're an insider who happens to have the right training or knowledge, you can cause a lot of damage,” Schwartz continued.

Finally, the speed by which access must be granted means that the military needs better auditing and monitoring tools than ever before. Traditionally, the military has relied on right-sizing the permissions associated with the access of insiders—generally, performing background checks and even lifestyle polygraphs or interviews with friends, neighbors and associates. But most of the time, these controls are designed to apply the “principle of least privilege” or “need to know,” which states that every insider should be granted exactly the least amount of access to do their work, explained Steve Hawkins, vice president of Raytheon Information Security Solutions.

“In practice, that turns out to be very challenging because of the sheer quantity of controls required at times with all possible factors or variables,” he said. “For example, it could require as many as 3 million rules just to define which of 100 doors that 30,000 employees are allowed to use.”

As a result, in situations where rightsizing permissions takes too much time and the organization can’t risk the productivity hit associated with right-sizing permissions, more effective monitoring and auditing becomes critical.

## PROACTIVE DEFENSE

Traditionally, the military has dealt with security by using firewalls, intrusion detection and other network security tools, along with comprehensive background checks of personnel. And it has made great progress since the 1996 release of a scathing General Accounting Office report on the weaknesses and risks of DoD networks.

The department rose to the challenge and has come a long way toward protecting their networks from both external and internal threats, analysts say. But as the threats change, information becomes more ubiquitous and criminals grow more sophisticated, the military must make another leap, both in terms of outlook and technology.

“Traditionally, technology to address insider threats has been reactive: Bad guys dream up ways to infiltrate and eventually the good guys find a way to stop it. They can cause a lot of damage before they are stopped,” said Toney Jennings, chief executive officer of CoreTrace, a security vendor. Both technology and the military’s approach to security must shift from reactive to proactive, Jennings urged.

NetWitness’ Schwartz agreed. “It’s about moving toward a model that assumes there will be some inappropriate activity on the network at all times, and being able to sense that activity, model that behavior, and shut down the activity before too much damage occurs,” he said.

There are many types of technology that take that proactive approach. All are useful and valid, and by using several in concert with each other, defense agencies can go a long way toward protecting themselves against many types of insider threats.

SecureWorks, for example, offers a network- monitoring service that constantly scans the network for insider attacks. The SecureWorks Counter Threat Unit performs in-depth analysis of emerging threats and zero-day vulnerabilities and then provides early warning and actionable security intelligence tailored to the specific environment. The service also includes early warning to emerging threats, threat and vulnerability analyses, remediation information and recommendations, access to its threat and vulnerability database, malware analysis and a full complement of reports.

Raytheon SureView is a host-based insider risk management solution that proactively identifies and supports investigations of user violations so that organizations can proactively manage insider incidents. Collected data is viewed in video-like, near real-time replay that displays the user’s activity, including keys typed, mouse movements, documents opened or Websites visited. With video replay, man-hours are saved by quickly determining a user’s motivation and intent.

SureView can also prompt users to comment in real-time, automatically stopping actions such as copying to USB drives, and producing actionable information to enable conclusive issue resolution. Raytheon has supplied insider threat solutions across the Department of Defense and other intelligence agencies, and the award of a contract by the Defense Information Systems Agency (DISA) for the DoD Insider Threat Focused Observation Tool was recently announced.

“We have moved from the analog age, where accurately judging trustworthiness was accomplished through constant face-toface interaction, to a digital age where we’re lucky if we can attempt to judge trustworthiness based on a brief glimpse of an e-mail thread—from an analog age where rightsizing permission consisted of a big combination lock on a paper file cabinet, to having to digitally prescribe which of thousands of files a user should and shouldn’t have access to,” Hawkins said.

NetWitness, which started as an insider threat management solution for the intelligence community, is used by many defense organizations today, including the Army. The next-generation network security monitoring software captures all packets across the network and provides security analysts the ability to perform detailed data mining on the information. Components include NetWitness NextGen, which records data across the network and analyzes it; NetWitness Investigator, which provides a real-time view into network traffic; NetWitness Concentrator, which aggregates data hierarchically; and NetWitness Decoder, a configurable network recording appliance that allows users to collect, filter and analyze network traffic.

Raytheon Oakley Systems’ host-based SureView insider threat solution offers endpoint activity monitoring and control, integrated endpoint and network protection, DVR-like video replay technology and forensics, incident replay that focuses on context and user intent, and policy-based user activity monitoring that continues even when the user or PC/laptop is offline or disconnected. Files and transmissions are monitored before encryption, making it less likely that malicious acts are able to hide behind it.

Raytheon also offers professional services in the area of insider threats including systems integration and application development. Among other customers, DISA uses this tool to counter insider threats.

To prevent unauthorized software or code, along with any changes to the network or hardware, CoreTrace offers Application Whitelisting. The program allows organizations to specify exactly which applications a user may run, along with the system's settings. Nothing outside those specifications is allowed.

For ironclad password protection, some agencies turn to Cloakware's Password Authority, which provides a policy-driven approach to monitoring, managing and auditing access to sensitive information and resources. The result is an automated privileged password management solution that organizations can configure to their specifications.

When insiders may be unwittingly used as pawns, Intrepidus offers PhishMe, which protects against targeted phishing and whaling attacks that are used in e-mail-based schemes such as spoofed e-mails or counterfeit Websites that unsuspecting employees may be tempted to access. The software-as-a-service solution provides instant, targeted employee training on how to avoid such attacks. PhishMe is used by the U.S. Military Academy, Air Force Academy, Naval Academy and Coast Guard Academy.

For situations in which employees travel or work from places other than the office, Credant Mobile Guardian uses policy-based intelligent encryption, providing tighter security than full disk encryption. It does this by working with other intelligent encryption layers to protect data from both external and insider threats.

## VULNERABILITY ASSESSMENT

In addition to technology, a thorough assessment to determine what's missing from the technology equation can make a big difference. Many organizations turn to CERT's on-site insider threat vulnerability assessment, which aims to help organizations better understand their vulnerabilities and how to manage those vulnerabilities. The assessment addresses technical, psychological, process and policy issues, and is structured around information technology, human resources, physical security, business processes, legal, management, and organizational issues.

As important as technology is in fighting insider threats, however, it won't do the job if other important processes are in place. If employees don't know the organization's rules surrounding data access and controls, for example, they may fail to report suspicious access by another employee. Or if employees are tasked with duties that are too closely intertwined, such as both making changes to data and approving the change, there may be adverse consequences.

Therefore, experts recommend sufficient separation of duties, enforcing documentation practices and backup procedures, enforcement of strict password rules and controls, well-defined business processes, thorough and ongoing background checks, periodic security awareness training for all personnel, monitoring and auditing of all employee actions online, saving data for use in investigations, deactivating computer access following termination, and clear documentation of insider threat controls.

And more sophisticated technology is on the way. For example, the Air Force Institute of Technology last year said it was developing technology that will use data mining and social networking techniques to detect and stop insider security threats and industrial espionage. The technology would analyze e-mail activities or find people with interest in sensitive topics, or be used to detect people who feel alienated within the organization. ♦

Back to Top

KMI Media Group
15800 Crabbs Branch Way, Suite 300, Rockville, Maryland 20855-2604 USA
tel: 301.670.5700 · fax: 301.670.5701 · toll-free: 888.299.8292