# ADVICE+DISSENT: Managing Technology Network Anomalies

By Karen D. Schwartz | *letters@govexec.com* | *Government Executive* | July 15, 2005

E-MAIL THIS ARTICLE
PRINTER-FRIENDLY VERSION
COMMENT ON THIS STORY

*Agencies can ward off hackers by finding pattern shifts before the damage is done.*

Secretly, surreptitiously, a hacker has circumvented your computer system's security infrastructure, broken into classified files and shut down your network. Because the hacker was experienced enough to bypass your signature-based security methods, he was able to get what he wanted and bring your network to its knees before anyone even realized something was amiss.

Every federal agency has the requisite security - antivirus software, firewalls and signature-based protection such as intrusion detection systems - but none would have stopped this attack. Hackers keep up with the growing number of new methods to circumvent security.

Enter anomaly detection. Unlike traditional security methods, anomaly detection examines patterns of network use and the information that comes from those patterns. The data then is compared to expected norms to identify unusual or unauthorized activity. If anomaly detection had been used in this case, the hacker's methods and timing would have been compared to normal system usage, quickly determining that this user and his methods were unusual.

"The idea is to use technology to bring different data sources together and determine what's anomalous behavior - not because any one source is telling you that, but because there were multiple events that seem to be related, and when you draw rules against them or do some statistical analysis against them, they appear to be out of the norm," says Edward Schwartz, senior architect at netForensics Inc., an Edison, N.J., information security vendor.

Anomaly detection is best used when a large amount of traffic must be examined, says Carlos Blazquez, security operations manager at Telos Corp. in Ashburn, Va., which has implemented the technique for several federal agencies. "It ties together security and operations so you have the big picture and can determine what's normal behavior on your network. That way, you can observe behavior that's abnormal," he says.

Unlike intrusion detection systems - by far, the most common security method used by federal agencies - anomaly detection works in environments where the enemy is unknown.

"Attackers can turn your machines into servers that perform reconnaissance and command-and-control work associated with malicious code," Schwartz says. "For example, a machine that is normally a workstation might suddenly begin to act like a Web server or start transmitting thousands of megabytes of data outbound. [intrusion detection] won't pick up an outbound session like that if it's on a well-known port, but anomaly detection will take telemetry from firewalls, IDS, routers and switches, and specific anomaly detection devices and bring it all together, determining that combination of things constitutes an unusual occurrence."

Perhaps most important, anomaly detection takes time into consideration - a critical factor when trying to spot anomalous behavior. "It's about reaction time," says Adam Powers, director of technology with the advanced technology group at Lancope, an Alpharetta, Ga., anomaly detection vendor. "It's designed to quickly and effectively provide an early warning system for these new, undocumented attacks."

## ACTIVE MONITORING

Anomaly detection is gaining converts mostly in the private sector, but it has many potential applications in the federal government, says Vance Hitch, chief information officer at the Justice Department. Hitch also is IT security and policy liaison for the Federal CIO Council. "We see it used in the financial services world, where anomaly detection can model and develop a working profile of how you use your credit card so it can detect when it's being used differently," he says. "Similarly, in the federal world, you could use it to monitor the different patterns of usage for each user - which files they access, what times they do it, the frequency of access - and flag when they start varying significantly from it."

Anomaly detection also can help agencies enforce security policies, says Damon Hopley, director of security and software at Enterasys, a vendor of secure network technology in Andover, Mass. "Most government agencies have acceptable usage policies that determine when employees should be logged out or avoid surfing the internal net, or whether FTP servers are run within the internal network," Hopley says. Some systems offer both passive and active monitoring, reacting and enforcing actions based on discovered anomalies or behaviors, he adds.

Some agencies already use some form of anomaly detection, but Hitch expects the technology to