

# CREDIT UNION JOURNAL

CUjournal  
COM

THE NATION'S LEADING INDEPENDENT CREDIT UNION NEWSWEEKLY

Vol. XII, No 47 November 24 2008

## TECHNOLOGY REPORT

# No-No To Nano

By Kevin Jepson, *Technology Correspondent*

CLINTON, Md.—iPod users can no longer get their groove on at USPS Federal Credit Union here—not since the CU rolled out a network event manager that alerts the IT manager of a potential breach—and then acts to stop it.

“People still don’t get that when they hook up an iPod, they can invite a member breach,” said Alan McHugh, IT manager at the \$190-million CU. “It can drive you insane.”

That’s because employees may get more than just 1,000 songs in their pocket when they hook-up iPods or other removable media to the network—they can also maliciously or unwittingly download thousands of credit union files. In fact, common belief has it that insiders pose the greatest risk when it comes to data loss.

“Most fraud happens from the inside,” said McHugh. “Our policy is that no hardware removable devices are allowed.”

Security managers report that data loss to insiders has dissipated, and that network abuse by insiders is now the most prevalent security issue, according to the 2007 Computer Crime and Security Survey conducted by the Computer Security Institute and the FBI.

Although data loss to external threats may be getting worse, internal breaches still result in a greater number of compromised records, countered a recent Verizon study.

Whether the issue is network abuse or data loss, USPS FCU automatically controls internal—and external—breaches with the TriGeo Security Information Manager (SIM). Two years ago, USPS FCU installed the client on 138 workstations and servers, said McHugh. The SIM appliance offers real-time log management, event correlation and endpoint security



with “active response” technology.

SIM continually collects the system logs from the hoard of network appliances at the CU and analyzes them “in seconds,” according to custom rules and 650 prebuilt rules, said Michelle Dickman, CEO at Post Falls, Idaho-based TriGeo.

“Monitoring logs now is a breeze,” said McHugh. “Before TriGeo, it was hell on earth. We had to manually go through each log on all of our appliances and servers.”

But automatic monitoring isn’t enough, he said. If a rule is tripped by a certain threatening network event, such as an iPod hook-up or a

brute-force attack on the network firewall, McHugh has configured TriGeo active response to instantly “kill” the event. TriGeo also instantly sends an alert to his cellphone or e-mail.

“I can tell TriGeo to notify me if it sees any FTP or telnet programs firing on any of my workstations, and kill the programs at the same time,” he explained. “TriGeo takes an automatic action just about everyday, and I’m glad. If you have to take the action yourself, it may be too late.”

The ability to automatically take action is unique among Security Information and Event Management products, said Dickman. “Other products can’t take action because they only drive the data to a database, populate the database and then run queries. So, they can only tell you after-the-fact that something happened. The TriGeo architecture also processes the events in memory, correlates in memory and takes a response in memory.”

TriGeo is the best deal, with mid-market competitors selling products at an average of \$90,000, Dickman said. That’s compared to an average of \$37,000 for an organization using TriGeo to cover hundreds of network sources, she said.

Alerts that report brute-force attacks are “invaluable,” McHugh added. “Even when I’m at home I can look to see what’s happening. If the ‘deny’ log shows hits flying into the network like nobody’s business, I can capture the attacker’s IP address. I’ll call the Internet Service Provider and report the IP, and I can set up my own deny list and stop the attacks at the router.”

TriGeo establishes a “complete forensic trail,” he said. “I can drill down in any event to find out what the network user was trying to accomplish.” □