

# Vulnerability assessment keeps airline flying

**CASE STUDY:** eEYE'S RETINA SECURITY SUITE FINDS, PLUGS NETWORK HOLES BEFORE TROUBLE HITS

By Anne Chen

**W**HEN THE W32.SASSER.WORM HIT THE INTERNET LAST MONTH, CONTINENTAL Airlines Inc.'s security team was able to find and plug its vulnerabilities before the worm could do any damage.

As other enterprises rushed to contain the havoc caused by W32.Sasser, the Houston-based airline ran vulnerability assessment scans using Retina Security Suite software from eEye Digital Security Inc. The software looked for the weakest links in the network by scanning all Continental Airlines' firewalls,

routers, servers and clients for vulnerabilities before they could be exploited, according to Andre Gold, director of information security at Continental Airlines.

Retina also provides Continental Airlines' security managers with an aggregated look at their network assets.

"What I wanted was a good view of what all my assets were in the company," Gold said. "I didn't need the patch management view; I needed the intruder's view. Now I know our susceptibility to attacks like the Sasser worm and can get hourly updates if I want."

Like Continental Airlines, enterprises across the country are turning to vulnerability assessment tools to mitigate security risks. Realizing the critical need to centralize and oversee security practices to ensure corporatewide network reliability, many organizations are conducting routine vulnerability assessments.

Continental Airlines wasn't always this well prepared. The sixth-largest U.S. air carrier learned its lesson the hard way in January last year when the SQL Slammer worm hit its corporate networks and disabled the ticketing system, causing flight delays.

Once Continental got its networks back up and running, the airline looked into deploying vulnerability assess-

ment tools, Gold said.

Continental leverages multiple IT providers for its technology services. For example, network monitoring is handled by Electronic Data Systems Corp., which, in turn, outsources some WAN monitoring operations to MCI Inc.

In addition to keeping outsourced operations in line, Continental's IT managers have their internal assets to monitor and manage. This is a fairly standard practice in many larger companies, but it can lead to interoperability issues.

For example, Continental Airlines uses Microsoft Corp.'s SMS (Systems Management Server) to deliver security patches, while outsourcer EDS uses eTrust from Computer Associates International Inc. to do the same. As a result, before the vulnerability assessment software was deployed, Continental Airlines never had a complete view of which assets were being managed or which devices had been patched for security vulnerability but still needed rebooting.

"Exposure, as it related to the information we had, didn't really correlate our exposure to the unknown," Gold said. "And with a worm with the payload of Slammer, the unknown in itself could potentially be the proliferation point to use to take your infrastructure down."

After the Slammer onslaught, Gold

knew he couldn't take any chances. Two years ago, when Gold was still running the IT end of the airline's e-commerce division, he deployed eEye's Retina Version 4.9 vulnerability assessment software to audit the airline's Web site. The program worked so well that Gold decided to deploy the software company-wide and unleashed 15 Retina vulnerability scanning engines into Continental's computing infrastructure. (Continental declined to say how much it spent on the eEye software.)

## Case file

- ▶ **Company** Continental Airlines
- ▶ **Location** Houston
- ▶ **Issue** Develop a way to determine the company's level of exposure to viruses and Trojan horses; provide enterprise vulnerability assessment for all technology assets, including those managed by third-party groups
- ▶ **Solution** Deploy vulnerability assessment software that gives security managers at Continental the ability to determine which assets are at risk when security threats arise; aggregate reports for an enterprise-wide view of vulnerabilities
- ▶ **Tools** eEye Digital Security's Retina Network Security Scanner, Retina Remediation Manager and REM Security Management Console; Microsoft's Windows and SQL Server
- ▶ **What's next** Test and pilot eEye's Blink Vulnerability Prevention System across the airline

Source: eWEEK Labs reporting

The result: a view of all assets on the corporate network, regardless of whether a particular machine is managed by Continental or an outsourcer.

Continental aggregates the feeds and speeds from its audits in eEye's REM Events Manager, which gives Gold a centralized repository from which to build executive reports. These reports can be accessed via a Web portal, which Gold can use to deliver targeted information pertaining to a particular asset to the business unit that is handling the monitoring and patching.

Currently, Gold and his team are working to automate some functions of REM Events Manager so that IT managers companywide can



**Andre Gold: "Now I know our susceptibility to attacks."**

have alerts sent directly to their e-mail in-boxes.

"I have the ability to go to my boss and give an exact statement on our susceptibility," Gold said. "For us, it makes sense to look at vulnerability as it relates to operational units within the organizations. We want all holes closed by the organi-

zations that manage those assets."

When the W32.Sasser. Worm attacked Continental, Gold employed REM Events Manager to determine his company's overall susceptibility to the outbreak. Using the vulnerability assessment suite, he quickly discovered which machines still needed to be patched or rebooted and alerted the operations staff or business group that is responsible for those machines.

Continental Airlines provides service to approximately 150 cities in the United States and 120 international destinations.

Gold is most concerned with securing machines at the airline's corporate headquarters, in Houston; within

data centers at major hubs such as Newark, N.J., Cleveland and Houston; and at Continental's reservations center, also in Houston.

With Continental encouraging passengers to purchase e-tickets, the potential for problems when viruses attack self-check-in machines that run Windows-based operating systems becomes much greater.

"This is why having risk-based and vulnerability information on all those assets is critical," Gold said. "When a virus comes out, I now have the ability to tell my senior managers exactly what our risks are at each location, as well as the potential of being taken down by an exploit from a vulnerability assessment and operational perspective." e

Reprinted from eWEEK, June 28, 2004 with permission from Ziff Davis Media Inc.

©2004 Ziff Davis Publishing Holdings Inc. All rights reserved.

## About eEye Digital Security

eEye Digital Security is a leading developer of security software and an active contributor to network security research and education. eEye provides complete vulnerability management solutions that address the full lifecycle of security threats: before, during, and after attacks. eEye's award-winning products include vulnerability assessment, remediation management, intrusion prevention and network forensics solutions. eEye protects the networks and digital assets of more than 2,500 corporate and government entities in over eighty countries. Founded in 1998, eEye is a privately held, venture-backed firm with headquarters in Orange County, Calif.



eEye Digital Security®

eEye Digital Security

One Columbia • Aliso Viejo, California 92656 • United States

T: +1 866.339.3732 (toll free) • T: +1 949.900.4100 • F: +1 949.349.9538

Geneva: T: +41 22 718 7700 • London: T: +44 (0) 20 8956.2270

[www.eeye.com](http://www.eeye.com)