REAL WORLD CASE 4

Online Resources, Lehman Brothers, and Others: Managing Network Security Systems

Like many companies, Online Resources Corp. (www.onlineresources.com) has deployed network intrusion-detection systems, firewalls, and antivirus tools on its networks. But until it installed a security event management suite, the company had a hard time dealing with the deluge of data pouring in from its various security systems. Not only were the incoming data voluminous and highly unreliable, but the IT staff also had to collect it from each system and then manually correlate it. The Security Information Management suite from NetForensics has changed that by automating the process of gathering, consolidating, correlating, and prioritizing that data, says Hugh McArthur, information security officer at the online bill processor. "It has given us a single place where we can go to get the information we need," he says.

The ever-increasing number of security tools and appliances around the network perimeter has created a stream of data that needs to be analyzed and correlated, says Michael Engle, vice president of information security at Lehman Brothers Holdings Inc. (www.lehman.com) in New York. Intrusion detection systems (IDS), intrusion prevention systems (IPS), firewalls and antivirus software, as well as operating systems and applications software, can detect and report an enormous number of security events daily.

For instance, the security incident management system at Lehman gathers and analyzes information about more than 1 million events from 15 different systems daily, according to Engle. This includes data from IDSs and authentication systems, a telephone password reset system, and an anomaly-detection system, as well as logs from Lehman's main e-commerce, Windows, and Unix systems. By year's end, the firm hopes to have an improved system in place that will help it gather and analyze more than 80 million daily events, including consolidated firewall log data.

Security information management tools typically "normalize" the security events data they collect by converting them into a common format and automatically filtering out duplicate data, such as multiple entries for the same virus attack. The normalized data are then dumped into a central database or repository, where correlation software can match data from different systems and look for patterns that might indicate an attack or threat. Finally, threats are prioritized based on their severity and the importance of the systems that are vulnerable. Data that suggest an attack against a critical e-commerce server, for instance, would be given a higher priority than an attack against a file server.

IT security administrators can view the information using a Web- or Java-based console, or dashboard, or the system can be configured to send alerts to pagers or other devices. Dashboards can give companies a real-time snapshot of what's going on inside the corporate network. "We are able to see events happen more quickly. It allows us to react faster if we see some activity bubble up in our systems," says White.

The benefits of deploying such software can be enormous, Engle says. When Lehman first installed an IDS in 1999, it generated more than 600 alerts daily—most of them false alarms. Today, thanks to the event-correlation features of its management system, administrators receive fewer than 10 per day. The system today is "turning more than 1 million events down to less than 10 alerts," Engle says. Such technology allows companies like Lehman to pinpoint threats far more efficiently, identify trends that might indicate an emerging threat, and fine-tune incident response.

The data that centralized event management systems capture and store are also useful for forensic analysis of network intrusions, says Nitin Ved, chief operating officer at NetForensics (www.netforensics.com). Such systems let companies drill down into the details of an attack, piece together relevant information from different systems, and quickly build a composite of events leading up to a security incident.

But as with any other technology, there are several major precautions, especially concerning the quality of the data that are fed into such systems. The old adage "garbage in, garbage out" holds true with such software, says Sweta Duseja, a product manager at security vendor Check Point Software Technologies (www.checkpoint.com). That's why it's important to ensure that the right filters and rules are set for capturing the information that's fed into the system, Engle says. For example, every time an end user on Lehman's network clicked on CNN's website, it generated 144 separate log events on Lehman's security systems, most of which were useless data. "Initially, we were sending too much data into the system because we thought that would put us in a better security position," Engle says.

Case Study Questions

1. What is the function of each of the network security tools identified in this case? Visit the websites of security firms Check Point and NetForensics to help you answer.
2. What is the value of security information management software to a company? Use the companies in this case as examples.
3. What can smaller firms who cannot afford the cost of such software do to properly manage and use the information about security from their network security systems? Give several examples.

Source: Adapted from Jaikumar Vijayan, "Corralling Security Data," *Computerworld*, August 18, 2003, pp. 28–29.