

Event Logs Are Key to a Secure Network

By Sari Greene

Gramm-Leach-Bliley Act regulations focus on safeguarding protected financial information. One of the most difficult requirements to comply with is the need to regularly and consistently evaluate and analyze the event and audit logs created by your bank's network and information technology devices. However challenging, this singular activity can yield enormous results. Suspicious, threatening and malicious activity is growing at an exponential pace on the networks of financial institutions, and these event logs often hold the key to discovering and halting harmful activity.

Most banks have smart people running well-designed networks that

of successful login events at a regional bank by a third-party service provider. Further investigation revealed that an untrustworthy employee of the third-party service provider was inappropriately accessing the bank's critical devices. Without log review, this activity may have gone unnoticed indefinitely; instead this information was used to close the breach.

There is an extensive criminal underground devoted to exploiting consumers by launching phishing attacks. The goal is to lure unsuspecting customers into providing sensitive financial information. A starting point is for the criminals to make replicas of a bank's Web site and modify the content. This activity is so common that many

and mistakenly assigned it an Internet-accessible address. This critical server contained sensitive customer information and was completely exposed to the Internet. The firewall logs indicated unusual inquiries directed to a previously unused network address. Sage Data Security analysts immediately notified the bank to bring the device offline.

These types of events are not uncommon. They happen every day, sometimes every minute, and no bank is immune. The key to solving the mystery in each of these situations was within the device audit logs. So why don't more banks catch these attacks? Part of the difficulty lies in the volume of event logs to review: each device generates approximately 600 events per minute. A network with 15 devices generates 13 million events per day to review. No matter how big the bank, few can afford to hire enough people to evaluate that volume of information.

There are a growing number of tools to monitor event logs, but while they might catch an overt situation, the reality is that successful log review requires both people and time, in addition to the right tools. Every bank needs a comprehensive understanding of what normal, baseline activity looks like, as a basis of comparison with new activity. Banks need to understand what information to capture, what to measure it against, and how to tell the difference between a blip and a true threat. The combination of a robust, event-log-management tool set with ongoing human intelligence insures network security. ◆

“Suspicious, threatening and malicious activity is growing at an exponential pace on the networks of financial institutions, and these event logs often hold the key to discovering and halting harmful activity.”



use sound policies and procedures. Yet they still experience threatening situations every day, some initiated by malicious intent, and others due to simple human error. Sage Data Security analysts review hundreds of logs daily on behalf of financial institutions nationwide. Consider the following incidents discovered and solved by the process of log review and analysis.

It has become commonplace for banks to outsource some, or even all, of their information technology infrastructure. During the course of daily log review, Sage Data Security analysts identified a disturbing trend

bank sites are mirrored multiple times a week. It's difficult to spot this activity using standard Web reports, since the technique that criminals use appears as if someone is simply viewing Web site pages. Using the data contained in Web site and firewall logs, Sage Security analysts correlate activity in order to identify the common precursors to an attack. This information can then be used to proactively stop an attack.

Not all threatening activity is malicious – sometimes, people just make mistakes. In one case, a programmer installed a new application on an e-commerce server

Sari Greene is the founder of South Portland, Maine-based Sage Data Security (www.sagedatasecurity.com), which secures financial institutions nationwide with its nDiscovery Security Information Management service. For more information, e-mail sari@sagedatasecurity.com.