Realtime publishers

"Leading the Conversation"

The Essentials Series

PCI Compliance

sponsored by

ALERTLOGIC

by Rebecca Herold

Copyright Statement

Using PCI DSS–Compliant Log Management to Identify Attacks from Outside the Enterprise

By Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI

Meeting the PCI DSS requirements for logging benefits businesses by putting into place logs that help to reveal when unauthorized users from outside the network perimeter, and any enterprise system, have breached security. There are many indicators within logs that are typically overlooked but could be used to more effectively keep hackers from successfully attacking network resources and compromising sensitive data. By establishing log management practices to identify, mitigate, and prevent network attacks, information security and IT practitioners will also be providing actions to support PCI DSS compliance.

Outside Attacks Impact Business

Network and database compromise by hackers and other malicious folks outside the organization can have a devastatingly negative impact on the business. Consider the following incidents that have recently occurred:

- Reported March 23, 2008—Hackers got into the Western Carolina University system and accessed personally identifiable information (PII) of alumni, including Social Security Numbers (SSNs), names, and addresses. The compromise was discovered while the school's network administrators were searching for all the PII storage locations so that they could remove the PII from the unsecured servers. The compromised server, "normally used for sharing class notes and assignments," had a history of being hacked "several times" in recent years. (Retrieved March 26, 2008 from http://www.citizen-times.com/apps/pbcs.dll/article?AID=/20080323/NEWS01/80322062.)
- Reported March 17, 2008—Hannaford Brothers supermarket chain reported that credit and debit card numbers were stolen during card authorization processing, possibly as the result of an application's vulnerability, putting around 4.2 million of their customers at risk of fraud. Approximately 1800 cases of fraud related to this hacking incident had already occurred by March 17. (Retrieved March 26, 2008 from http://www.wmur.com/news/15621249/detail.html.)

Other organizations can help to prevent these and other types of outsider compromises, or catch them before damage is done, with effective log management practices targeted at identifying outsider attacks.

PCI DSS Log Compliance Mitigates the Outsider Threat

PCI DSS log management requirements mitigate the threats from outside the organization in multiple ways. The logs can be used to:

- Determine individuals accessing data—in particular, cardholder data for PCI DSS—and identify access attempts from outside the network
- Identify intruder access to network files by examining logs for combinations of such things as
    - User identifiers and associated activities
    - Date and time of access to PII and sensitive data and resources
    - Type of access events and attempts to these resources
    - Affected data, system, and/or resource
    - Associated changes found in other logs
    - Time stamps and clock synchronization

Organizations can use file integrity monitoring and change detection software on logs to ensure existing log data cannot be changed without generating alerts. Outsiders often try to cover their tracks by removing logs that could point to their infiltration; the alerts will notify organizations as soon as the culprits try to remove evidence.

Using Combinations of Logs to Protect Against Outside Attacks

Ben Rothke, CISSP, QSA, and Senior Security Consultant at BT INS, reveals that, in his experience, firewall and router logs are the best indicators of attempts of unauthorized access from outsiders. These logs can not only show the dates and times of the access attempts but also, and perhaps more significantly, the source of the attack. However, he indicates that it is common during his PCI DSS audits to find log management activities woefully lacking in checks for these activities.

Annarita Giani, Postdoctoral Fellow in the Electrical Engineering and Computer Sciences Department, University of California at Berkeley, has done extensive systems log research and offers some good advice and insights into using logs to identify and defend against attacks from outside the enterprise.

> *Only a single log or alert does not provide enough information about an outside attack to be able to help defend against it. Attacks are more sophisticated nowadays, so more sophisticated approaches must be used to detect them.*
>
> *Here is an example. Usually an outside attacker does not want to be recognized. Public web servers are easily accessible from the Internet, so they are often used as a stepping-stone to other attacks. By doing a scan on a web server, a hacker can discover and exploit a vulnerable PHP web application. Also, a remote shell open from the web server to the attacker on an unusual port can allow the attacker to escalate his privilege and install a rootkit. Now the stage is set, and not only can the real attack to a third machine take place, but the connection with the attacker will be hard to find. So the basic steps of the attack include:*
>
> 1. *Privilege escalation*
> 2. *Creation of a fake account*
> 3. *Installation of a rootkit*
> 4. *Replacing system libraries with some backdoor versions*
>
> *While the logs for each of these steps separately do not represent the complete attack, their combined sequence is a sign of a remote shell through web application exploit. This is key; looking at more than one log to see what combinations of logs indicate outside attacks.*
>
> *It is important to know that only one source of data does not allow the detection of outside attacks. Finding malicious activity depends enormously on the ability to associate, in a meaningful way, diverse information, malicious or suspicious traffic, together with unexpected file modification.*

Effective log management practices to defend against the outsider threat must involve more than just simple review of isolated log entries. By developing procedures to identify key combinations of log entries, organizations can help to prevent hacks that could have damaged the business and compromised PII; in addition, they are supporting PCI DSS log management compliance.

A Practitioner's Perspective

A.B., an IT security expert practitioner with more than 25 years of experience within large multi-national companies (A.B.'s corporate rules do not allow him to have his name or his company's name published; however, his great expertise and vast experience offers some valuable lessons to readers), offers good points about how he has successfully used logs to help identify and prevent attacks originating from outside his organization.

> *There aren't usually messages in the logs that immediately suggest exploitation of a particular vulnerability. For example, obvious signs of remote command execution don't usually exist in the logs. Instead, look for signs in the logs of unusual behavior. Those are the things that suggest something is amiss. For instance, seeing a server inexplicably rebooting in the logs could be a symptom of the server being compromised and the hacker attempting to cover his tracks. Or it could be a failed buffer overflow attack that corrupted the operating system's memory and caused the crash. Of course, there could be of a bunch of non-malicious explanations, too.*
>
> *Another possibility is a log entry that shows an export of 1,000,000 credit card records. Is that normal? Probably not. That could be a hacker stealing credit card data. Even if the data is encrypted, the organization was hacked. Or, something even more subtle would be a log entry showing Rebecca Herold attempting to access customer data at 3:00am. But, you know she NEVER works those hours; that's suspicious. Maybe that is a bad guy using her username and password. Another example is the firewall logs showing users browsing to strange IP addresses. Perhaps that is a sign of a cross-site scripting or other web-based attack.*
>
> *Sometimes what you do *NOT* find in a log can be suspicious. For example, a server not logging when it should be could be a sign of a hacker erasing log entries or disabling the system logs.*
>
> *Something else that is important for log management is following through to investigate suspicious logs in a timely manner. The lawyers I work with during hacking incidents are emphatic that when you find something suspicious in logs, you *MUST* investigate it in a timely fashion. Ignoring suspicious behavior in logs is far worse than not logging at all. It is also important to document your investigations to show auditors that you are diligent about reacting to notable log entries.*

As you can see, A.B.'s experience supports Annarita's research as well as the practices Ben looks for as a QSA.

Be Prepared for Your QSA and Protect Against Outside Threats

Most outside attacks leave some kind of trail. The trick is in knowing how to find these intrusions among thousands, or even millions, of normal log entries. The key to success is to start with high-level queries of specific types of logs and associated activities, then work your way down to more specific conditions. Of course, this task would be too overwhelming without automation. Use log correlation tools to monitor network activity in real-time to identify when there is any suspicious or inappropriate access and usage occurring that originated from outside the network.

When creating your log management procedures to detect outside attacks, consider creating procedures to look for combinations of the following:

- Firewall logs that show unexpected or abnormal activities
- Router logs that show unexpected or abnormal activities
- Logs that reveal privilege escalation on certain accounts
- Logs that reveal creation of a fake account
- Logs that indicate installation of a rootkit
- Logs that show system libraries have been modified or replaced, possibly with some backdoor versions
- User identifiers/accounts and associated activities that do not make sense for the associated job responsibilities—Was a user on the network, or accessing a financial application, at an unusual or unexpected time? Were there an excessive number of failed login attempts?
- Logs showing date and time of access to PII and sensitive data and resources
- Logs for terminal services login attempts; check logins to all public terminal servers and check for successful logins from unrecognized IP addresses
- Logs specifying the type of access events and attempts to resources—specific to PCI DSS, what financial resources were accessed?
- Logs that indicate affected or modified data, in particular, financial data
- Logs that show access or changes to systems, particularly financial systems and associated resources
- Logs that show time stamp and clock synchronization tampering from outside sources

- Logs that show connections from outside the enterprise lasted for lengths of time beyond what is normally expected
- Logs showing source and destination IPs and ports—Who was talking to whom? And over what ports? Is anything unusual about the communications? Are the times of the connections out of the ordinary?
- Logs showing protocols used—Was the connection a TCP, UDP, ICMP, or other protocol? Were any of them out of the ordinary?
- Logs that show the number of packets sent and received—Was there abnormal packet activity in correlation to the connection that was made? Look at the packet payload size. How much data was involved in this connection? Is this unusual, unexpected, or abnormal?
- Logs containing TCP flags—What TCP flags were in use by both client and server in the connection? What TCP flags are outside the boundaries of what would be expected as normal?

Do not consider this a comprehensive list but rather a starting point to help you identify the logs to use within your organization. These practices will not only help protect your business network but also support PCI DSS log management requirements.

Summary

Keep in mind that when you are preparing for a PCI DSS audit, it is typical for the QSA to examine your log records along with your log management procedures. The QSA will look to determine whether your procedures are effective for identifying attacks from outside the enterprise, and she will determine whether you have been following your policies and procedures consistently and reacting appropriately to suspicious combinations of log entries that indicate possible outside attacks.

Sound log management practices not only help protect your business from attackers outside your network but also support PCI DSS compliance.