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 Insider Access Abuse

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

Meeting the requirements for PCI DSS logging benefits businesses by putting into place logs that help to identify when authorized users may be doing things they should not be doing. There are literally thousands of types of logs that can be generated on corporate networks and appliances. Unfortunately, too few information security and IT practitioners understand that there are very important differences in how to use logs to identify insider threats from other types of threats. Too few know how to review the logs to identify when authorized users may be doing inappropriate activities with their access. The indicators found within logs for insider abuse are largely much different than indicators for other types of threats.

How the Insider Threat Impacts Business

Think about how many people have authorized access to information resources within your organization. These "insiders" often include:

- Employees
- Contract workers
- Temporary workers
- Business partners
- Consultants
- External auditors
- Customers
- Former employees whose access has not been removed

Think about the sensitive information these insiders have been authorized to access. Think about all the bad things a malicious insider could do with this access. If there are gaps in security controls, malicious insiders can take advantage of those vulnerabilities to use the access privileges of authorized insiders.

The huge Société Générale fraud scandal is a good example of how insiders can exploit control gaps and have a devastating impact on the business. In early 2008, Jerome Kerviel, a Société Générale employee, was accused of stealing computer passwords, sending fake email messages, and illegally accessing the bank's computer system to exceed trading limits and cover up his actions. Kerviel allegedly bought futures contracts but did not follow requirements to offset them with countervailing buys. He reportedly did this by gaining unauthorized computer access, possibly through his co-workers' accounts or by exploiting control vulnerabilities, and forged documents that made it look like he had offset purchases, circumventing risk controls. His actions cost the company $7.5 billion. It has been widely discussed that better controls, including effective log management and review procedures, could have prevented this unprecedented internal fraud of this magnitude.


There is a 72% chance that the next successful network attack will come from an insider. - ICSA Labs

PCI DSS Log Compliance Mitigates the Insider Threat

PCI DSS log management requirements mitigate the insider threat in multiple ways. The logs can be used to:

- Validate that proper controls are in place
- Validate policy compliance
- Determine when individuals are accessing data in ways that are beyond their authorized use of the data for business responsibilities
- Determine whether access is inappropriate based upon criteria such as:
  - Access to audit trails and associated modifications
  - Invalid logical access attempts
  - Use of identification and authentication mechanisms
  - Time stamps and clock synchronization changes
  - File integrity monitoring and change detection software for logs to ensure existing log data cannot be changed without generating alerts

Using Logs to Protect Against the Insider Threat

Ben Rothke, CISSP, QSA, and Senior Security Consultant at BT INS, points out that, in his experience, database logs are the best indicators of the insider threat because they clearly show when authorized users have been snooping around in files that they have no reason to be accessing at particular times or in order to perform their business responsibilities.

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 insider attacks.

> *It is estimated that the majority of all computer security breaches are due to insider attacks. While some insider attackers use simple methodology, others rely on more sophisticated approaches, such as inserting a toolkit, an agent or scanning the network. Since the inside attackers have some authorization, they are able to compromise somebody else's account to launch the attack and be virtually invisible.*
>
> *As organizations move to more automated environments, it becomes possible to detect signs of insider misuse much earlier than has previously been possible. In fact, information systems can be instrumented to record all uses of the system, down to the monitoring of individual keystrokes and mouse movements. A technologically adept malicious insider, however, may be aware of these countermeasures and take actions to neutralize them.*
>
> *Many attacks can be detected using a combination of logs; log analysis of multiple log entries usually must be done to detect insider abuse. The first step is to build models of an insider attack. Once the models are built, compare them with the system logs. This can be done manually, but it becomes very difficult if the number of models is high. And in any case the amount of logs quickly becomes unmanageable.*
>
> *Using only one source of data does not allow the detection of insider attacks. Finding nontrivial malicious activity depends greatly upon the ability to log and associate diverse information, malicious or suspicious traffic, and unexpected file modification.*

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 some good points about how he has successfully used logs to identify the insider threat.

> *Look for signs in the logs of unusual behavior. Those are the things that suggest something is amiss. For instance, something subtle would be a log entry showing an employee attempting to access customer data at 3:00am. But, she NEVER works those hours - that's suspicious. Maybe that is a bad guy using her username and password, or maybe the employee is trying to commit fraud.*
>
> *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 an authorized user erasing log entries or disabling the system logs.*
>
> *It is important for the IT personnel to become familiar with logs. How do you become familiar with logs? Simple; read them, even when you have a few spare minutes or are on a horribly boring conference call. It won't take long to start recognizing normal behavior as opposed to possible suspicious behavior. The secret is not to look for specific log entries, but to look for entries that stick out like a sore thumb.*

Annarita provides more advice based upon her research with real life incidents.

> *It is common for malicious insiders to use an encrypted connection, such as a Virtual Private Network, to commit their crimes. Remote access is mostly used by attackers that have system privileges but do not have direct access to their computer at work, or by attackers who are no longer employed; they may have been fired, so they cannot enter in the building, but their access to the information system still exists. Remote access logs together with file access logs are very useful proofs of insider attacks that occur outside the facilities. Another method technical insiders often use is to spoof the source IP address to try and cover their identity.*

A large number of organizations fail to quickly remove remote access capabilities from individuals with whom they have terminated their business relationship. Many never remove the access at all! I know of dozens of cases in which vindictive ex-employees continued to use their remote access capabilities to do harm to their former employers.

Competent PCI DSS QSAs will closely review your personnel exit and termination policies and procedures, along with your user account logs, to ensure you consistently remove systems and information access as soon as possible following—and in some especially risky situations, before—the employee departure.

Be Prepared for Your QSA and Protect Against Insider Threats

Ben Rothke indicates the log management portion of the PCI DSS audits he performs is significant compared with the other PCI DSS requirement reviews. According to Ben, "Companies are finding that they can't simply install an appliance and suddenly be PCI compliant. Logs require an organization to really understand their infrastructure. Far too many organizations have no idea about what and how much logs they are generating. PCI log requirements are a rude awaking for them."

It is important for organizations preparing for a PCI DSS audit to know that QSAs typically examine the actual log records themselves to determine whether there is anything suspicious or unusual. Ben indicates that he not only takes and examines samples of data from the logs identified as being critical to financial transactions but also reviews the log management policies and procedures to ensure that the logs he reviews are in compliance with the policies and procedures.

The common log management problems Ben finds when performing PCI DSS reviews include:

- Completely misconfigured logs
- Default log settings left unchanged from installation
- Wrong items being logged
- No one reads the logs
- No one follows up on log issues
- Logs not correlated to any threats or vulnerabilities

> 🕮 According to the CERT/Secret Service Insider Threat study, in 74% of incidents and frauds committed by insiders, the insiders' identities were obtained using system logs (Source: "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," Carnegie Mellon CERT and U.S. Secret Service, 2004, http://www.cert.org/archive/pdf/bankfin040820.pdf.

The bottom line is that organizations must establish a well-documented log management program to not only meet PCI DSS log requirements but also help identify, and often prevent, damage that could occur from prolonged access from the insider threat.

The following list highlights just a few of the logs that are helpful for organizations to use to identify the insider threat and to be in compliance with PCI DSS:

- Remote access logs
- RADIUS authentication logs
- File access logs
- Database logs
- Application logs
- Email logs and application logs for authenticated email (POP, IMAP, etc.)
- IP address logs
- Authentication logs
- Windows system and Active Directory (AD) login/logout activity logs
- UNIX SSH login logs
- FTP server logs
- Logs indicating passively sniffed chat and IM login processes

Do not consider this a comprehensive list but rather a starting point to help you identify the logs to use within your organization. This type of documentation will also be important for ensuring PCI DSS compliance.

Summary

History has taught us that most malicious insiders will attempt to take steps to conceal their actions. The insiders who know that the logs can be used to identify them will typically attempt to hide their fraudulent actions by modifying the logs, and it is not unusual for them to try to change the logs in such a way to implicate someone else for their devious actions. Sound log management practices not only help to fight this insider threat but also support PCI DSS compliance.