

Watch Your Logs!

By Christian Malatesti

Security logs provide administrators with an invaluable means of monitoring the security of the system and identifying operational problems.

Security logs contain information about events occurring within the network systems and applications of an organization. They are comprised of a number of log entries, each referring to details pertaining to a specific event, and provide administrators with a invaluable means of monitoring the security of the system and identifying operational problems. They record user actions, perform auditing and forensic analyses, and detect security incidents such as policy violations. In addition, the review of security logs is strongly recommended by federal regulations such as the FISMA, GLBA, BSA, SOX, HIPAA and Payment Card Industry Data Security Standard.

Policies and procedures

Organizations must create and document formal policies, standards and procedures for log management activities. This practice promotes a consistent approach towards log management throughout the organization and ensures compliance with laws and regulations. Essential topics addressed in these documents include review process, retention period, location of online and offline logs, and the staff in charge of reviewing the log records.

Configuration

The security logs of all network components – operating systems, subsystems such as databases, program change systems and applications – should be active and monitored. Administrators need to determine the information to be logged and estimate how much space the log will require. Sufficient resources should be allocated in order to ensure that the logging information is not overwritten. Typically, the space allocated should allow for the capture of online logging information for a period of five days after which a backup is created for offline storage.

Data retention requirements mandate that organizations maintain copies of log files for a minimum of three months. Also, current industry best practices recommend that the logs be retained for a period of six months in order to support computer or network crime investigations that the organiza-

tion may have to face. In order to comply with these requirements and to ensure confidentiality and integrity of the log information, offline logs should be stored in a secure location with a strong physical access control mechanism.

Review

Security personnel and network administrators usually manage network and security devices and thus, they need to analyze the log information and report issues to management. Typically, administrators review logs once a week. However, it is highly recommended to review logs on a daily basis. Organizations also need to monitor administrators' actions to ensure accountability and reduce the probability of internal criminal activities. This can be achieved by enforcing dual control, i.e., by having more than one person review the logs.

There are two main approaches to review a security log:

- Real time reviews – the software applications that analyze the logs notify the administrators about any unusual event as soon as it occurs.
- Batch mode reviews – a report is generated periodically so that it can be analyzed at the administrators' convenience.

While reviewing security logs, the most challenging activity is “event correlation” which refers to the identification of common factors between two or more log entries. Event correlation usually requires statistical tools to discover patterns that would normally be overlooked by the human eye. However, human knowledge and experience are essential to interpret the results of the tools and distinguish the false positives from the significant findings. Event correlation requires administrators to ensure that the event time stamps collected from the systems involved in the analysis are synchronized and that sufficient logging activities are available.

What information?

The format of a security log may vary depending on the source of the log. Logs generated by security software such

as antivirus software, firewalls, intrusion detection systems, or authentication servers may differ from those created by operating systems or applications. Log formats may also be vendor specific. This lack of standardization, combined with the large number of log information sources, produces inconsistencies and incompatibilities in content and format that make it difficult for administrators to analyze the collected data. This is the reason why some organizations utilize automated methods to consolidate multiple logs into a single standard that can be easily analyzed.

Regardless of the format and source, all logs should record at least the following activities:

- User logins and logouts
- Configuration changes
- Administrative account logins and logouts
- Failed access to critical folders and files
- Changes to users, groups and services
- All suspicious activities such as:
 - Switching user ID during an online session
 - Guessing passwords
 - Attempting to use unauthorized privileges

Regulatory Compliance

Organizations needing to comply with federal legislation and regulations must review log information on a regular basis. The requirements for each regulation are discussed below.

Federal Information Security Management Act

The motivation behind FISMA was to secure computer systems and networks within the federal government and its affiliates. The FISMA Act requires federal agencies to develop, document, and implement an organization-wide program to provide information security for their information systems.¹ Security log retention and review are a significant part of the overall security requirements. *NIST SP 800-53, Recommended Security Controls for Federal Information Systems* defines several controls for proper log management that are part of the compliance requirements with FISMA.

Gramm-Leach-Bliley Act

The GLBA requires financial institutions to protect non-public customer information from unauthorized access and use.² Security logs can be used by organizations to detect security incidents affecting customer information. In the case of an incident, a financial institution can determine which customer's information has been accessed in an unauthorized manner by reviewing its logs. The institution now has the option of notifying only those customers that are affected, or could be affected under the judgment of reasonable possibility. In the absence of such a mechanism to single out affected customers, the institution is required to inform all the customers.

1 <http://csrc.nist.gov/policies/FISMA-final.pdf>.

2 <http://banking.senate.gov/conf/fintl5.pdf>.

Health Insurance Portability and Accountability Act

HIPAA requires healthcare organizations to protect personally identifiable health information.³ These organizations would be greatly benefited by regular reviews of audit logs and access reports. Software systems dealing with medical information need to generate detailed audit information that describes how a user accesses and utilizes resources. HIPAA also requires that logs are backed up on a regular basis and retained for at least six years.

Sarbanes-Oxley Act

Organizations requiring compliance with the SOX Act would need to review their logs on a regular basis to detect potential security breaches and retain records of log reviews for future assessments by auditors.⁴ Organizations would do good to record relevant system events such as shutdowns, restarts and any other unusual events. Additionally, the SOX Act requires log information be kept confidential and disclosed only to authorized personnel.

Payment Card Industry Data Security Standard

The PCI DSS requires all organizations that process and transmit credit card information to monitor access to the network resources and card holder information.⁵ Logging and audit trails must be enabled and need to be unique to each entity's cardholder data environment. This provides for timely forensic investigation in the event of a computer crime or fraud. Compliance with the PCI standard applies to merchants and service providers regardless of the method of payment (telephone, e-commerce, mail, etc.).

Bank Secrecy Act

Banks are subject to stringent anti-money laundering laws such as the Bank Secrecy Act of 1970, which establishes that banks must maintain records and report all suspicious activities to law enforcement agencies.⁶ Banks that do not meet stipulated requirements may be subject to fines of up to \$1 million a day. Logs are a reliable source to identify money laundering activities since they can be used to trace the source and the routes of money transferred over the Internet. Hackers can take over an innocent server to send out cash transfer orders and masquerade as another person. However, logs would fingerprint the activities of the hacker on the server as well as the actual origin of such activities. The trail of transactions across all the servers on the Internet can then be used by forensic investigators to track down the hacker.

Conclusion

Logs serve as one of the primary sources of information for system administration support. The importance of log reten-

3 <http://aspe.hhs.gov/admsimp/final/PvcTxt01.htm>.

4 <http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf>.

5 https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf.

6 <http://www.uhuh.com/laws/31usc1051.htm>.

tion and review is highlighted by the log management requirements imposed by the numerous laws, regulations and standards governing organizations in different industries. These requirements serve to provide organizations with the impetus to monitor logs. Compliance aside, it is the responsibility of every organization to monitor network, system and application activities to ensure the highest level of security of confidential information and this should be reason enough to implement log management.

Recommended readings

— *Guide to Computer Security Log Management*, NIST SP 800-92, <http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf>

About the Author

Christian Malatesti is a consultant with Enterprise Risk Management, one of the leading providers of IT Security and Risk Management services to local, national and international businesses. He can be reached at cmalatesti@emrisk.com.