CMSGu2014-05

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Audit Log Management

CERT-MU

National Computer Board
Mauritius

Version 1.0

November 2014

Issue No. 5

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of these guidelines is to provide advice and principles regarding the use of audit logs, the content of audit logs and the actions that are required as a result of a specific auditable event action occurring.

1.2 Audience

The target audience for this guideline includes computer security staff and program managers; system, network, and application administrators; computer security incident response teams; and others who are responsible for performing duties related to computer security audit and log management.

1.3 Document Structure

This document is organised into the following sections:

Section 1 contains the document's content, the targeted audience and the document's structure.

Section 2 presents a background on the need for audit logs.

Section 3 elaborates on the audit log management process.

Section 4 highlights the general principles for audit logs.

Section 5 concludes the document.

Section 6 contains a list of references that have been used in this document.

Appendix A defines a set of acronyms used in this document.

2.0 Background

Organisation can benefit from audit logs in several ways. Audit logs help to ensure that computer security records are stored in adequate detail for an appropriate period of time. Routine log reviews and analysis are beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems shortly after they have occurred, and for providing information useful for resolving such problems. Audit logs can also be useful for performing forensic analysis, supporting the organisation's internal investigations, establishing baselines, and identifying operational trends and long-term problems.

Audit trails can be used in conjunction with access controls to identify and provide information about users suspected of unauthorised modification of data. Besides the inherent benefits of audit log management, a number of laws and regulations further compel organisations to store and review certain logs.

Below are two examples of standards that help define organisation's needs for log management, especially in the financial and payment card industries

- **Sarbanes-Oxley Act (SOX) of 2002:**
  Although SOX applies primarily to financial and accounting practices, it also encompasses the information technology (IT) functions that support these practices. SOX can be supported by reviewing logs regularly to look for signs of security violations, including exploitation, as well as retaining logs and records of log reviews for future review by auditors.

- **Payment Card Industry Data Security Standard (PCI DSS):**
  PCI DSS applies to organizations that "store, process or transmit cardholder data" for credit cards. One of the requirements of PCI DSS is to "track...all access to network resources and cardholder data"

3.0 Audit Log Management Process

As part of the audit log management process, an organisation should define the roles and responsibilities of the users who are involved in the management and use of audit logs. Users involved in the management of audit records include:

- Business users
- Help desk / customer support
- Systems management users
- Contract management
- Internal & external auditors
- Security administrators
- Internal investigation teams
- Computer Security incident response team
- Law enforcement agencies

The needs of all potential users must be considered when designing audit facilities. Different users will have very different needs; for example, business users will have completely different needs than security administrators or investigation teams.

Organisations should:

- Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and
- Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Organisations should develop audit log policies that clearly define mandatory requirements and principles for audit log management. The policies should address who within an organization can establish and manage audit log infrastructures. Organisations should also ensure that policies, guidelines and procedures that have any relationship to audit logging should incorporate and support the appropriate audit log management requirements and principles.

Audit Logs held on any storage medium will record large volumes of data on a regular basis. This will impact the resources required to store the data for the appropriate length of time. Many logs have a maximum size and when this is reached the log might overwrite old data resulting in a loss of integrity and availability. It might be appropriate in some cases to record less information and maintain the log's integrity than record everything but be unable to guarantee integrity.

3.1 Events to be recorded

All business processes comprise of a number activities supported by information technology (IT). To protect and secure correct processing technical and security controls are in place and each of these controls can be linked to creating an entry in audit logs. To avoid the creation of "oversized" audit logs it is necessary to tailor audit log files to the needs of the organisation. This can be achieved by selecting the auditable events in the business processes of an organisation.

An auditable event in this specific instance is defined as a single event (within a business process) that could lead to the compromise of the integrity and/or security of an information system and therefore directly or indirectly compromise a business process. The consequences of such a breach could lead to data loss (theft), misuse of systems & privileges, or fraud. Defining what events should be audited and captured within an IT system, and the processes used to capture such events, is analogous in the real world to placing surveillance cameras on important physical sites to detect activity and to record it for future action. The number, volume and variety of auditable events has increased greatly, which has created the requirement for security event management – the process for generating, transmitting storing, analysing and disposing of security log data. Security event management helps to ensure that security records are stored in sufficient detail for an appropriate period of time.

3.2 Audit Tools

Many types of tools have been developed over the past few years to enable organisations to automate the collection and reporting of the large number of audit events that may occur. It is very possible that millions of audit record s could be generated every day as a result of payments across a host of devices, e.g. network devices, security devices, mobile devices , and physical access, servers, desktops, databases . In order to be able to manage the security and risk the development of a central point of collection and analysis is essential. The use of

automated tools to help this process is essential. An example of this type of tool is Security information and event management (SIEM) technology.

SIEM provides real - time monitoring and historical reporting of security events from networks, systems and applications. SIEM deployments are helpful in addressing regulatory compliance reporting requirements. SIEM could also be used to improve security operations, threat management and incident response capabilities. The requirements for compliance reporting, log management, user and resource access monitoring, external threat monitoring, and security incident response should be defined. This may require the inclusion of other groups in the requirements definition effort, including audit/compliance, IT operations, application owners and line - of - business managers.

SIEM technology provides:

- The collection, reporting and analysis of log data (primarily from host systems and applications, and secondarily from network and security devices) — to support regulatory compliance reporting, internal threat management and resource access monitoring. It supports the privileged user and resource access monitoring activities of the IT security organisation, and the reporting needs of the internal audit and compliance organisations.
- The processing of log and event data from security devices, network devices, systems and applications in real time to provide security monitoring, event correlation and incident response. It supports the external and internal threat monitoring activities of the IT security organisation.

In addition to syslog and SIEM software, there are several other types of software that may be helpful for audit log management. Host - based intrusion detection systems (IDS) monitor the characteristics of a host and the events occurring within it, which might include OS, security software, and application logs. Host - based IDS products are often part of a log management infrastructure, but they cannot take the place of syslog and SIEM software. Other utilities that are helpful for audit log management include visualisation tools, log rotation utilities, and log conversion utilities.

3.3 Fields to be recorded

The information systems should produce audit records that contain sufficient information to establish, at a minimum,

- what type of event occurred, e.g. the server, system process, ip address, mac address etc.,
- when (date and time) the event occurred, e.g. time stamps where the event occurred,
- where from the origination of the event occurred , e.g. source and destination addresses, user/process identifiers ,
- where to the ev ent occurred, e.g. the identity or name of the affected data, system or component, • the outcome (success or failure) of the event, e.g. event descriptions, event integrity, success/fail indications and
- who the identity of any user/subject associated with th e event was , e.g. a signature verification process, an IDS, an AV system, a firewall, a payment transaction record etc.

Additional data may be recorded for some events, for example, the identity of the target user where systems management access is being made to their account; a transaction reference number where a single transaction is being tracked across multiple systems. Accurate timing is crucial to the usability of audit logs, particularly where logs are maintained across multiple distributed platforms. Audit logs may contain intrusive and confidential personnel information. Appropriate privacy measures should be taken.

4.0 Audit Log General Principles

The following audit logging principles are generally recommended:

4.1 Audit System design

1. Audit facilities should be designed with their specific use(s) in mind, not simply adapted from existing system logs.
2. Organisations should create and maintain an audit log management structure, including policy, procedures, rules and tools.
3. Where a single business or system transaction will result in the creation of audit data on multiple systems, design consideration should be given to how the complete audit information about that transaction will be collated and made available to a ”user of the audit logs”.
4. Organisations should provide appropriate support, e.g. training, provision of appropriate tool s, for all staff that will be making use of the audit logs.
5. Audit log files should be periodically saved and moved to another storage space. The periodicity may be influenced by the classification of the data, but should be defined either according to a fixed size (e.g. every time the log reaches 1Mb) and / or according to a fixed period of time (e.g. per day, per week).
6. Attacks on systems should be prevented by the use of technical preventive controls. These controls should be preferred above procedural preventive controls if possible. Both measures should be used in conjunction with examination of the audit data.
7. Organisations should consider the use of a Security Event management system due to the large volume of security events.
8. Organisations should not solely rely on unauthorised events or breaches of policy, but should additionally consider proactive monitoring.
9. Organisations should consider the use of Security information and event management (SIEM) technology to help the automation and collection of auditable events.
10. All audit records should contain a time stamp. Ensure that each system’s clock is synched to a common time source so that its timestamp will match those generated by other systems.
11. The privacy of personal data should be protected.
12. Measures should be implemented in order that deleting or modifying logs of own activities should be detected and alerted immediately.
13. Administrators should not be able to erase or de - activate logs of activities.

14. Audit events should be protected from modification by using digital signatures to sign audit records.
15. Audit events should be archived to ‘write - once ‘media to protect the archive from modification or deletion.
16. Where audit records are subject to cryptographic authentication the input data to the authentication computation should include an accurate timestamp.
17. Archived audit log files should be protected by appropriate logical and physical security mechanisms.
18. The capture of customer sensitive data in audit logs should be avoided. If necessary sensitive data should be masked, tokenised or encrypted to avoid data breaches.
19. Where audit data are encrypted, the appropriate decryption software and keys must be available and properly maintained, under appropriate access control, for the whole of the lifetime of the encrypted data. Proper maintenance should include periodic testing and adequate back - up to cater for loss of stored encryption keys.
20. Audi t records should be created in a simple standard format.
21. Where audit data are compressed, the appropriate decompression software must be available and properly maintained for the whole of the lifetime of the compressed data. Proper maintenance should include periodic testing.

4.2 Management of audit logs

1. The ownership of audit data should be clearly defined.
2. Audit records should be classified at a level commensurate with the classification of the systems and data they are intended to protect.
3. Changes to programs or the configuration of programs (e.g. Job Control Language) that generate audit logs should themselves be logged in an independent change log.
4. Periodic independent tests should be made to assure that all events that are expected to be logged are actual ly included in the logs.
5. Access to the source code and configuration files of logging programmes should be protected from access by the originator of the events being recorded.
6. The set - up of log programs and procedures should be documented and properly app roved and tested.
7. Audit logs should include the registration of any period of time during which logging has been disabled.
8. Audit logs should be named using a clear, explicit and efficient naming convention.

9. The storage location of audit logs should be chosen such that access to the logs can be made within a clearly defined response time.
10. Security - related audit records should be protected from modification or deletion by recording the originator of the event. Changes of security related audit records should be traced by recording the originator of the changed event.
11. System administrator and auditor privileges should not rest with the same individual.
12. Those responsible for reviewing audit records should not have sufficient privilege to be able to originate the events that are recorded.
13. Auditors and anyone authorised to access audit logs should only be granted read - only access; only specific applications & systems which require it should have write access to audit logs.
14. Unauthorised parties should not be able to manipulate processes, files, or other components that could impact audit logging.
15. Routine review of audit logs by human operators should be established in a manner which is commensurate with the risks to the system being protected.
16. Where systems producing audit data are outsourced, the contracting party should define an appropriate access policy for the third party.
17. Audit log files should be periodically saved and moved to another storage space. The periodicity may be influenced by the classification of t he data, but should be defined by the retention period.
18. The integrity of transferred Audit logs should be verified. This could be done by message digests for each audit log file.
19. The archived Audit logs should be appropriately protected. Unauthorised physical access should be prevented. Appropriate environmental controls should be applied to prevent damage to the media.
20. Audit data which are backed - up should be subject to the same level of access control and the same level of security measures as the original data.
21. Ensure that the backup of the audit data is tested on a regular basis to ensure that it is still readable.
22. Audit logs should be disposed of in a fashion commensurate with their security classification.

4.3 Retention Period

1. Organisations should ensure that audit retention is part of the organisation's overall retention policy.

4.4 Application and use of Audit Logs

1. Where the execution of sensitive security - related actions cannot be made subject to dual control, then that execution should be monitored in a timely fashion.
2. An organisation should determine which data is classified as audit data and should protect and preserve this data appropriately.
3. Personal notes should be kept by incident investigators throughout the whole course of an investigation and those notes should themselves be protected and preserved in the same manner as audit data.
4. Audit records used during an investigation must be preserved at least until the end of the investigation and for any subsequent prosecution irrespective of their normal retention period.
5. Follow the organisation's incident response policy to investigate an audit log incident.
6. System configuration information should be modified, if necessary, to prevent an event from overwhelming the system.

5.0 Conclusion

Audits logs are beneficial in many ways. However, the collection, correlation and review of log data can be a daunting task. Where feasible, auditing tools should be used to minimize manual processing overhead. Moreover, audit system design, log retention period and log application and use are important elements to be considered during an audit log management process

5.0 References

- **http://www.europeanpaymentscouncil.eu**
- **http://www.csun.edu**
- **http://delhi.gov.in**
- **http://csrc.nist.gov**

Appendix A

List of Acronyms

AV	Anti-virus
IDS	Intrusion Detection System
IT	Information Technology
OS	Operating System
PCI DSS	Payment Card Industry Data Security Standard
SIEM	Security Information and Event Management
SOX	Sarbanes-Oxley