Lebanese American University

Information Security Regulations

Log Management and Monitoring Regulations

Last Updated: May 2017
Version 1.2

Overview

Logging from critical systems, applications and services can provide key information and potential indicators of compromise. Although logging information may not be viewed on a daily basis, it is critical to have from a forensics standpoint.

Purpose

The log management and monitoring regulations define the requirements for managing and monitoring the logs that are generated by LAU computer and communications systems handled by the IT Department.

Scope

The log management and monitoring regulations apply to all LAU production computer and communications systems managed by the IT department.

Regulations

General Requirements

All servers, network and security appliances shall record and retain, where applicable, audit-logging information sufficient to answer the following questions:

- What activity was performed?
- Who or what performed the activity, including the IP of the system the activity was performed from (subject)?
- What the activity was performed on (object)?
- When was the activity performed?
- What tool(s) the activity was performed with?
- What was the status (such as success vs. failure) outcome, or result of the activity?

Sensitive Application Systems Logs

All production application systems that handle LAU information must generate logs that capture every addition, modification, and deletion to such sensitive information where applicable.

Log Management Infrastructure

LAU management must provide the budget and tools necessary to support a log management infrastructure.

Physical Access Logging

LAU will maintain logs of all physical access to protected areas, including electronic physical access systems and maintain logs when these systems raised alarms.

Privileged System Command Accountability and Traceability
All privileged commands issued on servers, network and security appliances must be traceable, where applicable, to specific individuals through the use of comprehensive logs.

Systems Log and Audit Trail Disclosure
Systems logs or application audit trails must be classified as CONFIDENTIAL and not be disclosed to any person outside the team of individuals who view such information in order to perform their jobs or investigate information security incidents. All exceptions require the approval of the VPHRUS.

Computer and Communication System Logs
All LAU production servers and communication systems must log events, at a minimum, production application start and stop times, system boot and restart times, system configuration changes, system errors and corrective actions taken.

Logging Security-Relevant Events
All servers, network and security appliances must securely log all significant security relevant events including, but not limited to, password guessing attempts, attempts to use privileges that are not authorized, modifications to production application software, and modifications to system software.

Log Access Logging
Access to all system logs and audit trails on LAU computer and communications systems must be logged.

Log Initialization Logging
The initialization of all system logs and audit trails on LAU computer and communications systems must be logged.

Systems Software Utilities
Access to systems software utilities must be restricted to a small number of trusted and authorized users and logged whenever these utilities are executed.

Security Incident and Event Management (SIEM)
LAU must employ security incident and event management software to facilitate the collection, storage, correlation and analysis of systems logs. It must make all LAU log data available in human readable format, must have tools to report on events found within event logs and must normalize the events coming from all devices into a unique format. All production servers and devices under the IT Department supervision should forward all logs stated before to the SIEM.

Log Retention Period
Every log and audit trail produced by a LAU computer or communication system, stored on SIEM, must be retained for one year.

Clock Synchronization
The time setting on all LAU computer and communications systems must be kept current using a known, stable version of Network Time Protocol or similar technology.