CENTRE FOR CYBER SECURITY

Guide

Logging – part of resilient cyber defence

Logging –magnifying glass to the past

Contents

Introduction 3

How to read this guide 3

What to log, and where 4

- Domain Name System (DNS) servers 4
- Dynamic Host Configuration Protocol (DHCP) 4
- Firewalls 4
- Authentication servers 4
- Routers 5
- Virtual private network (VPN) 5
- Web servers 5
- Web proxy 5
- Anti-malware systems 6
- Email systems 6
- Other types of logs 6

Log management 7

- Log generation 7
- Log collection 8
- Storage of logs 8
- Use of logs 9
- Log deletion 9

CENTRE FOR CYBER SECURITY

Kastellet 30
2100 København Ø
Tel: + 45 3332 5580
Email: cfcs@cfcs.dk

Frontpage illustration: Pasieka/Science Photo Library/Ritzau Scanpix

3rd edition July 2023.

Introduction

With logging enabled, it is possible to rewind time. The Centre for Cyber Security and IT security companies often come across organizations whose logging procedures are inadequate, thus making it difficult to identify the source and impact of security incidents. Lessons learned from handling IT security incidents in a number of organizations have demonstrated the importance of logging as a key element in IT security incident analysis.

Logging is the backbone of a resilient cyber defence, as it helps to "identify possible IT security incidents. This guide is intended to help organizations ensure sufficient logging to facilitate incident management. Logging is an integral part of the continuous efforts to plan, implement, monitor and improve cyber security.

How to read this guide

This guide is divided into two sections: A list of areas where logging is recommended and an outline for management/governance considerations.

Included in the list are the systems and devices from which a log is typically required during incident response. Logging is a useful tool when suspected or actual information security incident has been identified.

This guide is meant for both the governance level as well as the implementation level. The guide can also be used as a guideline for supplier management requirements.

In addition to the systems mentioned in this guide, logging is possible in a number of different areas. Some logs may be interesting from an operational perspective, as they may help identify errors, optimize resources, etc. This guide deals with logs from an IT security incident management perspective, and the highlighted logs are those most interesting from an incident analysis perspective.

This guide does not cover topics such as log analysis and the protection of logs.

Useful log sources

The organization should log all recursive Domain Name System (DNS) servers
Recursive DNS server logs are important to determine which internal system (clients, servers, etc.) have inquired about which domain names and the time of the query. Logging of DNS queries can be used to identify malware communication with a Command & Control server (C2-server).

Organization must as a minimum log:

- Universal Time Coordinated (UTC), timestamp.
- Source IP address.
- DNS queries with content and responses.

The organization should log all internal DHCP-servers (Dynamic Host Configuration Protocol)
Logs from DHCP-servers are necessary to track which internal units (for example clients) has used the specific IP address at a given time.

Organization must as a minimum log:

- UTC
- Assigned IP address
- MAC address

The organization should log data traffic in and out of the organization (firewalls)
When analysing cyber-attacks, it is interesting to examine the patterns of legitimate network traffic, thus providing a complete picture of an organization's network traffic. Thus, it is important that all traffic (allowed or denied) passing an organization's firewall and/or other traffic filtering devices, is logged.

Organization must as a minimum log:

- UTC
- Source/destination IP address and port
- Decision (for example approval, blocking or closing of connection)
- Amount of data sent and received in the session's traffic.

The organization should log all authentication servers
With regards to authentication servers (For further information visit Microsoft, 2021), two types of events in particular should be logged to provide a basis for subsequent analysis:

1. Events that seem suspicious - even if they only occur once. For instance, if a regular user account is added to a restricted group, as the group membership is updated.
2. Accumulation of one-time events that exceed a specified threshold. For instance, an unusually large number of failed login attempts followed by a successful login may indicate a successful brute force attack. Conversely, though, numerous failed login attempts could also be a sign of a failed brute force attack.

Organization must as a minimum log:

- UTC
- Type of event
- Account name
- Source IP address
- Source hostname
- Verdict – result of the attempted login(s).

The organization should log all internal routers

Routers can be configured to allow or block different types of network traffic based on access policies. Routers capable of blocking traffic should be configured to log the handling of traffic.

Organization must as a minimum log:

- UTC
- Source/destination IP address
- Port
- Decision (for example – whether the connection was blocked, approved or shut down).

The organization should log all client Virtual Private Network (VPN) gateways

When users access an organization's systems remotely (for example when working from a home office or while travelling), logging will contain information useful to uncover where the connection came from, and to what extent a user was granted or denied access. It can reveal attempts to compromise the remote access, and can be used in compilation with other log data.

Organization must as a minimum log:

- UTC
- Extern IP address
- Username
- Assigned IP address
- Failed and approved logins.

The organization should log their Internet-facing web servers and web services based on HTTPS (for example, websites, APIs and MQ)

Some attackers use web servers to obtain or maintain access to a network, for example through websites or webmail services and web APIs. The web server log can help investigate the actions of an attacker. If web servers are behind proxy / load balancer, it is important to resolve the original client IP address.

Organization must as a minimum log:

- UTC
- Source's external IP address
- URIs
- Return codes
- Referrer
- User agent
- Amount of sent and received bytes.

The organization should log other Internet-facing services (for example, FTP and SSH)

Other Internet-facing services can be a target for the attackers as well, and therefore activities there should be logged. Which activities that are relevant to log depend on the type of services. Log data from Internet-facing services can reveal compromising of user accounts, the software used, available contents, configuration settings etc.

Organization must as a minimum log:

- UTC
- Source's external IP address
- Relevant activity for the service.

The organization should log all web proxy servers

If a web proxy is used for outgoing Internet traffic, the log can help to identify potentially malicious domain names and queries from compromised devices.

Organization must as a minimum log:

- UTC
- Client's IP address
- Method (GET, POST etc.)
- URIs
- Return code
- Hostname and user (if possible).

The organization should log events on all anti-malware systems

Logs from Antimalware sandbox systems, Anti-virus (AV), Endpoint Detection and Response (EDR) and Intrusion Detection System (IDS) can help to create an overview and timeline of attempted attack as well as, for example, attempts to run a specific malware. All quarantined files should be saved for later analysis.

Organization must as a minimum log:

- UTC
- Activity (for example, quarantine or blocking)
- Process / File name / Activity that causes the event.

The organization should log all email systems, including inbound and outbound gateways, and spam/virus filtering services

Email system logs, including logs from in- and outbound email gateways and spam/virus filtering services, can help detect and investigate phishing attempts, malware delivery, and certain exfiltration techniques.

Organization must as a minimum log:

- UTC
- Sender/recipient email addresses
- Name and IP address of source/destination gateways
- Subject line
- Size of the message
- Names of the attached files.

The organization should log other elements than network components
In addition to the logs mentioned above, a number of other logs could be relevant in an investigation of IT security incidents. The following elements should be considered:

- Logs on individual clients
- Logs on critical file servers
- ”Success” and ”failure” audits logs across platforms
- Logs from privileged account management software and password management suites
- Logs of administrative logins and actions
- Logs from application whitelisting solutions and blocked PowerShell scripts
- Logs from industrial control systems.

Different log collection and configuration management tools are available, and should be chosen based on the organization’s needs, the current threat landscape and security incident response needs. The choice of tools and the level of logging details should be determined in close dialogue with security incident managers.

Prior to log collection, the organization must consider how the logs will be managed. Some of these considerations are outlined below.

Log management

Logging policy should be defined by the organization based on the ability to get the maximum benefit from the logs generated, and to use them for analysis. The policy should define the purpose and principles of logging and be used to establish the procedures required to ensure adequate and accurate logging.

The logging policy and procedures should describe log generation, collection, storage, retention periods, proactive and reactive log analysis, as well as deletion of logs. The policy and procedures should be coordinated with those responsible for security incident handling, whether they are in-house security personnel, a government agency, or a security company contracted to investigate potential IT security incidents. The policy and procedures should ensure that the available log records are accurate, readable and go sufficiently far back in time.

One way to establish adequate policies and procedures is to prepare scenarios of possible IT security incidents that an organization would like to be able to analyse. (ISO 2015).

Log generation
Risk assessments are a good starting point. If resources require prioritization then the organization should continuously assess which logs are relevant.

Risk assessment should be conducted taking the organization’s mission/business operations, vulnerabilities and the prevailing threat landscape into account; not all logs are equally important from a cyber security point of view. In addition to the identified risks, an organization may have to abide certain rules, laws, industry standards, etc.

For instance, an organization may have to comply with special logging requirements, including which data may not be logged, how long logs may be stored etc.

When an organization has performed its risk assessment, the following steps need to be in place in order to get the best out of its logging procedures:

- Establish an overview of which logging rules the organization has to comply with.
- Create an overview of the IT architecture (topology) supplemented with a diagram.
- Prepare descriptions of all Internet connection points and the rules governing them (such as firewall rules).
- Make a list of all DNS and DHCP servers, as well as VPN concentrators.
- Document all log policy implementations, including e.g. Group Policy Objects that define the log policies.
- Make sure that the log level is sufficiently detailed and contains the information required to investigate an incident. It has to be aligned with the organization policy.
- Check that the correct client IP address is logged and not the IP address of, for instance, a proxy or load balancer.
- Establish an overview of all generated logs. Many logs are generated on single systems and used in daily operations, but could be valuable in the overall cyber security logging capability. It requires the right understanding of the individual log types.
- Make sure to specify to your suppliers which logs need to be generated and how to access these logs (CFCS, 2023).
- Ensure sufficient log storage capacity in accordance with retention policies defined by the organization. This should be automated.

Log collection

The purpose of this guide is to improve the analysing capability of organizations concerning IT security incidents. Consequently, the Centre for Cyber Security recommends that organizations establish a system capable of storing logs from multiple sources in a central location. Here is a list of some of the elements to include in log policies and procedures:

- Time stamps are essential. In order to ensure that logs in central log systems and on decentralized devices can be used for subsequent analysis, it is vital that the log records use UTC time stamping, synchronized with a central time server;
- Data integrity is a must. It is important to mitigate the risk of log data manipulation when logs are generated on individual systems, transferred to a central logging system, and when stored in a central repository. It is equally important to mitigate the risk of deleting, manipulating or adding data to the logs (ISO 8.2, 2022) by employees with privileged rights, external partners or attackers;
- Documentation is key. Organizations should prepare documentation showing the log sources and what kind of data is logged. This will allow third parties to gain an overview of what kind of data is available in case of a potential security incident.

Test of logs
Remember to test logs continuously. When logging is enabled, it is important to test that the data is logged correctly, the right data is saved, and - that it is stored as long as defined by the organization policy. It is also important to test if the necessary information is available in order to investigate a potential security incident. Is it possible to identify who has done what, and when? Involve security incident responders in your evaluation.

Storage of logs
A cyber-attack is not always detected while in progress, emphasizing the need to store logs.

Cyber-attacks may go undetected for weeks or months. Therefore, organizations need to decide on log retention periods. The decision on how long data has to be stored should be based on an individual risk assessment and in compliance with relevant regulation, which in some cases lays down rules for how long the logs must be stored before they are deleted. These aspects should be reflected in the log policy. The logs should be stored for a minimum of 13 months, unless the law requires otherwise. In all cases, The Centre for Cyber Security recommends that logs are stored for a minimum of 13 month.

Organizations must ensure that the right security measures are implemented to protect the integrity, confidentiality and availability of stored logs. This means that logs need to be protected on the same level as other sensitive information, and that any unauthorized access is prevented. It should be ensured that no employees can manipulate the logs undetected.

Organizations have to consider how to back up log data. It is recommended that backing up of log data follows the same procedures governing other types of sensitive information, in accordance with the organization's security policy.

Use of logs
In addition to logs being a valuable tool when analysing IT security incidents, it is important to mention that in conjunction with monitoring it can also be used proactively for optimization of operations and for systematic detection of irregularities and inappropriateness in systems – thus enabling an organization to create situational awareness.

Organization policies and procedures for logging should specify how logs can be used. Should a specific log be analysed on a regular basis or only in case of security incidents? It has to be defined how review of specific logs is done, and what to look for. Procedures for log analysis should be established, and it should be decided whether to conduct the analysis manually, or with the support of an automated system, such as a SIEM platform. The Centre for Cyber Security recommend that log analysis is supported by appropriate tools.

Examining the logs periodically or in real time[1] may be agreed with an external supplier.

[1] Proactive use of logs is out of the scope of this guide.

Log deletion

When logs are deleted, organizations must ensure that logs are completely removed from all the media they were stored in, including decentralized devices (firewalls, etc.), backups, analysis platforms, etc. Deletion of logs should follow an established procedure. The procedure should be subject to regular compliance checks.

Recommendations

- The organization should log all Internet-facing services and central internal IT systems.
- The organization should centralize logging and storing of logs.
- The organization should use a common time source and same time zone (UTC).
- Logs should be stored minimum 13 months, unless legislation requires something else.

References

International Organization for Standardization (ISO). (2015).
*Information technology – Security techniques – Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues. (*DS/ISO/IEC Standard No. 27033-3).
https://www.iso.org/standard/51582.html

International Organization for Standardization (ISO). (2022).
Information security, cybersecurity and privacy protection — Information security controls. (ISO/IEC Standard No. 27002:2022).
https://www.iso.org/standard/75652.html

Microsoft. (2021).
Audit Policy Recommendations.
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations