EUROPEAN
COMMISSION

Brussels, 23.6.2020
C(2020) 4296 final

IT security standard

Logging and monitoring

CONTENTS

1. INTRODUCTION

Preventive controls can go a long way in assuring the security of CISs, but they cannot guarantee absolute security and might be circumvented/evaded. Detective controls need to be also in place to identify whether incidents impacting confidentiality, integrity and/or availability of such CISs have taken place so that corrective measures can be taken.

This supervision is performed through logging and monitoring. CISs used by the European Commission must record at least the basic security-related events in logs so that they can be monitored in (near) real-time and/or reviewed after an incident has occurred.

2. PURPOSE

This IT security standard lays down requirements for the successive phases in the lifecycle of the Commission's IT security log files:

- log generation;
- log management; and
- log monitoring.

2.1. Log generation

In case of an incident, the information captured within log files could be used as forensic evidence to trace the actions that have been taken by the attacker on the network and the systems. As such, it is important that information contained in log files contributes to correctly assess the impact of an incident. However, log entries should not contain unnecessary information in order to keep log files manageable. The content of log files should offer answers to the following questions:

- *Who*: the identity of the user and the type and origin of device used when generating the event[1].
- *Where*: the CIS on which the event is generated as well as the application or service on that system that is generating the event.
- *What*: the action(s) performed that triggered the event as well as whether that action was successful or not.
- *When*: the clear and precise timing on when the event took place.

2.2. Log management

Log files must be transferred to a central location at regular intervals. Controls must be in place to guarantee their integrity and protect them against tampering. Incidents are rarely detected immediately, so this standard stipulates how long the files should be retained.

[1] According to the Regulation 2018/1725 on protection of personal data.

2.3. Log monitoring

Log files come from various systems (e.g. servers and clients, network devices, applications) that each use their own format and structure. Files have to be standardised so that the central logging facility can process them, correlate them and make them searchable.

Once the log files have been centralised and made searchable, effective monitoring can take place. In order to detect anomalies, we first have to determine what constitutes normal behaviour of a CIS; this is referred to as 'baselining'.

It is also advisable to look beyond the log files. Sources such as security event reports from third-party applications or providers (e.g. cloud services) can provide additional input. This standard also addresses the use of these additional resources.

Due to the sheer volume of log files generated, their analysis should be automated where possible. It is important to establish the use cases (scenarios) that require monitoring and select input from the centralised log files to support generation of the relevant alerts. This standard provides an overview of the controls needed to generate meaningful alerts.

3. SCOPE

This standard covers IT security-related logging activities regarding all the CISs within the Commission IT environment, including:

- ✓ network layer – e.g. routers, switches, DNS, network and/or application firewalls, proxy servers and gateways, etc.;
- ✓ systems layer – i.e. all physical and virtual operating systems, including hypervisors and other appliances; and
- ✓ application layer – i.e. all applications and databases. IT systems for the application layer include AD, web applications, file systems, e-mails, knowledge sharing tools and databases.

4. EXCEPTIONS

The adoption of this standard is mandatory and an integral part of the Commission's information security policy. Exceptions must be handled in accordance with Article 2.2 of the IT security standard on "IT security compliance management" and the "implementing rules for Articles 3, 5, 7, 8, 9, 10, 11, 12, 14 and 15 of Decision 2017/46 on the security of communication and information systems in the Commission".

5. DEFINITIONS

For the purposes of this standard, in addition to the definitions in Article 2 of "COMMISSION DECISION (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission" and Article 2 of the "implementing rules for Articles 3, 5, 7, 8, 9, 10, 11, 12, 14, 15 of Decision 2017/46 on the security of communication and information systems in the Commission", the following definitions also apply:

5.1. Definitions

Term	Definition
anti-virus detect-only events	Cases where malicious software was detected but not cleaned.
anti-virus protection failures	Cases where the anti-virus software does not behave as expected, e.g. crashes, protecting engine unloads and update failures.
centralised logs	Logs compiled at the central logging facility.
central logging facility	Centralised entity where log files are gathered, processed and monitored.
cloud service provider	Company that provides one or more components of cloud computing – typically infrastructure as a service (IaaS), software as a service (SaaS) or platform as a service (PaaS).
data centre	A data centre is a building, dedicated space within a building, or a group of buildings used to house computer systems and associated components.
firewall	A network security system that monitors and controls incoming and outgoing network traffic on the basis of set security rules. Typically establishes a barrier between network segments or zones.
intrusion detection system (IDS)	Monitors network or host activity through analysis of patterns based on known attacks.
internet-facing system	A system that is publicly reachable from the internet.
intrusion prevention system (IPS)	Monitors network or host activity through analysis of patterns based on known attacks and blocks the violating traffic before it can reach its destination.
local logs	Log files stored on the device that generated them.
proxy	A system that intermediates between an end-user device (e.g. a computer) and another server from which a user or client is requesting a service.
secure configuration baseline	A set of basic security objectives which must be met by any given service or system.
web application firewall (WAF)	A firewall that monitors, filters or blocks data sent to a web application based on ISO/OSI model layer 7 logic.

5.2. Acronyms

Acronym	Definition
AD	active directory
CIS	communication and information system
CPU	central processing unit
DHCP	dynamic host configuration protocol
DNS	domain name system
HTTP	hypertext transfer protocol
IDS	intrusion detection system
IP	internet protocol
IPS	intrusion prevention system
NAT	network address translation
NIDS	network intrusion detection system
NIPS	network intrusion prevention system
P2P	peer-to-peer
SIEM	security information and event management
SMTP	simple mail transfer protocol
SOC	security operations centre
TCP	transmission control protocol
TLS	transport layer security
TOR	the onion router
UDP	user datagram protocol
URL	uniform resource locator
UTC	Coordinated Universal Time
VPN	virtual private network
W3C	World wide web consortium
WAF	web application firewall

6. LOG GENERATION

Rationale

The following factors mean that the generation of logs is subject to certain requirements:

- logs provide visibility on actions on a CIS and are the basis for detecting and/or investigating information security incidents;
- logs contain details of transactions on the CIS, enabling to determine their nature and origin;
- CISs hosted on Commission premises and elsewhere may contain important logs; and
- attackers may seek to alter or delete logs in order to cover their tracks.

6.1. Minimum log content

(M = mandatory, R = recommended)

S/N	Requirement	Implementation
1.	Each log file **shall** have at least the following information: *Who?* a. user identifier, provided it can be linked directly or indirectly to an individual (identity); b. service information, e.g. service name and protocol; c. source address (e.g. user's device identifier, IP address); *Where?* d. system/application identifier; e. system/application address (e.g. cluster/hostname, IP address, URL); *What* f. detailed event information, including affected object; g. event status (e.g. success/failure, reason for failure, denied/allowed); *When* h. date and timestamp of event, including time zone information; and i. date and timestamp of log entry (may differ from (h)).	M
2.	Logs **shall** not contain sensitive information (e.g. passwords), unless deemed necessary for the events being logged. Any sensitive information logged **shall** be limited to the minimum content required.	M
3.	In case logs contain personal information, they **shall** be processed according to the relevant regulation in force, they **shall** not involve more data than needed and related formal documentation **shall** be maintained.	M
4.	Business sensitive information **shall** not be logged without prior formal authorisation of the data owner.	M

6.2. General events

(M = mandatory, R = recommended)

S/N	Requirement	Implementation
1.	Every security configuration baseline **shall** include a section on logging that complies with this standard.	M
2.	Detected deviations from the logging configuration baseline **shall** trigger an IT security event and be investigated.	M
3.	Modification or deletion of log files and/or changes to the logging policy settings **shall** generate log entries.	M
4.	Log entries **shall** be generated for each system logon and logoff attempt.	M
5.	Log entries **shall** be generated for administration activities, including (but not only): a. creation, modification or deletion of accounts; b. creation, modification or deletion of groups and group memberships; and c. allocation, modification and removal of authorisations to accounts and groups.	M
6.	Log entries **shall** be generated for all password changes and resets.	M
7.	Log entries **shall** be generated for all other relevant security configuration changes.	M
8.	Log entries **shall** be generated for the creation, modification and deletion of services.	M
9.	For each system, the system owner **shall** determine, on the basis of a risk assessment, whether other activities should be logged.	M

6.3. Network device and security-specific events

(M = mandatory, R = recommended)

S/N	Requirement	Implementation
1.	Remote access communication **shall** be logged and monitored.	M
2.	Where IP addresses are dynamically assigned, DHCP leases **shall** be logged.	M
3.	The outbound proxy **should** log all users' web requests unless properly justified on the basis a risk assessment. The proxy log format **should** be compliant with the W3C standard.	R
4.	The DNS server **shall** log all DNS requests.	M
5.	Networking and network security devices **shall** generate log entries (where technically possible) at least for: a. attempts both successful and failed to access assets containing sensitive information; b. all blocked outgoing attempts to connect to networks outside the control of the Commission; c. VPN and other remote access authentications (both successful and failed); d. access both successful and failed to anonymisation services (e.g. TOR); e. file uploads to external web sites; f. file downloads, including content type; g. blocked proxy connections to prohibited content; and h. activation and deactivation of the device.	M
6.	Log entries **shall** be generated in the event of anti-virus protection failures.	M
7.	Changes to the configuration of network security devices and appliances, and the creation, modification and removal of user and access rights **shall** be logged. This includes, but is not limited to, security gateways, firewalls, IDS and IPS.	M
8.	Access to and security administration of cloud administration portals **shall** be logged and monitored, in line with the principles set out in this standard.	M

6.4. Operating system and database-specific events

(M = mandatory, R = recommended)

S/N	Requirement	Implementation
1.	At least the following system events **shall** be logged: a. system crashes, shutdowns and restarts; b. changes to operating system files (e.g. binaries and other key files). The files to be logged should be selected on the basis of a risk assessment; c. changes in permissions to access critical system files. The files to be logged should be selected on the basis of a risk assessment; d. software installations and updates by a CIS, an application or a user; e. database user activity; and f. capacity or limit exhaustion events for memory, disk, CPU and other system resources.	M

6.5. E-mail

(M = mandatory, R = recommended)

S/N	Requirement	Implementation
1.	E-mail traffic **shall** be logged in the form of message tracking to enable identification of the sender, recipients, subject, size of the e-mails and their attachments.	M
2.	E-mail attachment content types, names and sizes **shall** be logged.	M

6.6. Application-specific events

(M = mandatory, R = recommended)

S/N	Requirement	Implementation
1.	Log entries **shall** be generated in the event of backup failures.	M
2.	A risk assessment **shall** be performed for each application in order to determine additional logging requirements.	M

6.7. Other events

(M = mandatory, R = recommended)

S/N	Requirement	Implementation
1.	Log entries **shall** be generated when people enter or leave the data centre facilities.	M

6.8. Log timestamp synchronisation

It is important that the same synchronised date and time are used across the organisation as logs from multiple CISs might need to be combined in order to recreate the full story of events.

(M = mandatory, R = recommended)

S/N	Requirement	Implementation
1.	A minimum of two synchronized time sources **shall** be used by all systems and network devices to retrieve time information on a regular basis, hence ensuring timestamp consistency in logs.	M
2.	To limit an attacker's ability to alter the time source, a minimum of three synchronised time sources **should** be used to ensure timestamp consistency in logs.	R
3.	Timestamp information in log files **shall** include the time zone. If time zone cannot be included, system clock **shall** be set to UTC+0 (GMT)	M
4.	System clocks **should** be set to UTC+0 (GMT).	R
5.	Changes to the time synchronization configuration of a system or failure of time synchronization **shall** generate log events	M

6.9. Local log storage protection

(M = mandatory, R = recommended)

S/N	Requirement	Implementation
1.	Log files **shall** not be removed from the log source until they have been transmitted to the central logging facility. *See chapter 7 for more information on central logging facility.*	M
2.	Measures **shall** be taken to ensure log file contents are protected against modification and deletion.	M
3.	Log files at rest **should** be encrypted in line with Commission standards on cryptography.	R
4.	Under the 'least privilege' principle, only personnel responsible for managing and auditing local log files **shall** have access to them and with personal credentials.	M
5.	Where a system has to be restaged, the log files **shall** be backed up beforehand to prevent loss of information.	M

7. LOG MANAGEMENT

Rationale

The following factors mean that the management and handling of logs must adhere to certain principles:

- logs must be protected, as the loss or compromise of log information may hamper the investigation of IT or Information security incidents;
- proactive identification of potential IT security incidents is based on automated and manual log analysis, and thus requires the centralisation of logs;
- insufficient log information, especially as regards the history of activities on a system, may prevent complete analysis of an IT security incident; and
- logs may contain sensitive information (e.g. personal data) and must be handled in an appropriate manner both locally and in the central logging facility.

7.1. Log centralisation

(M = mandatory, R = recommended)

S/N	Requirement	Implementation
1.	Log files **shall** be transmitted to the central logging facility as soon as possible (near real-time) and at least every 15 minutes.	M

7.2. Protection of central logging facility information

7.2.1. Logs in transit

(M = mandatory, R = recommended)

S/N	Requirement	Implementation
1.	During transit, IT security log files **should** be encrypted in line with Commission standards on cryptography.	R
2.	Only protocols that ensure the reliable delivery of data **should** be used to transmit log files to the central logging facility, so as to ensure data integrity (e.g. preferring TCP over UDP).	R
3.	Where log files are transmitted, the identity of the source **should** be verified by the use of strong authentication.	R
4.	Wherever possible, incoming log files **shall** be verified against expected format and/or content, and any other applicable sign of potential tampering (e.g. missing lines in line-numbered files).	M

7.2.2. Logs at rest

(M = mandatory, R = recommended)

S/N	Requirement	Implementation
1.	Log files **should** be stored in an encrypted format in line with Commission standards on cryptography.	R
2.	A record of the activities on log files (i.e. accesses and actions) **shall** be kept by an independent role.	M

7.2.3. Access restriction

(M = mandatory, R = recommended)

S/N	Requirement	Implementation
1.	Under the 'least privilege' principle, only personnel responsible for managing and monitoring log files **shall** have access to log files in the central logging facility.	M
2.	Assignment of roles for the management of the log files **shall** follow the 'segregation of duties' principle.	M
3.	Accounts with access to log files and their associated access rights **shall** be periodically reviewed, in line with the authentication and access control standard.	M

7.2.4. Backup and restore

(M = mandatory, R = recommended)

S/N	Requirement	Implementation
1.	Log files **shall** be backed up and backups shall be tested regularly in line with the Commission standard on backups.	M
2.	Backups of log files **should** be stored off-site to mitigate data loss in the event of a disaster.	R

7.3. Log retention

(M = mandatory, R = recommended)

S/N	Requirement	Implementation
1.	Log files **shall** be kept at the central logging facility for at least 6 months, to ensure effectiveness of incident response;	M
2.	Log files **shall** be kept at the central logging facility for no longer than 12 months.	M
3.	Log files **shall** be deleted or anonymised after the retention period has expired[2].	M
4.	Where the content of the log file is subject to specific regulations or legislations, any retention periods stipulated therein **shall** take precedence.	M

7.4. Log disposal

(M = mandatory, R = recommended)

S/N	Requirement	Implementation
1.	Logs **shall** not be disposed of before expiry of the established retention period for the log file.	M
2.	Logs **shall** be disposed of on all relevant CISs, including: a. local log files; b. centralised logs; and c. log file backups (i.e. backups dedicated exclusively to log data).	M
3.	Subject to the application of specific regulations or legislations, where a system is under investigation, the log data **shall** not be removed, even after the retention period, until the event has been fully investigated and forensic evidence has been gathered.	M

[2] Both in the central and in the local logging facilities

8. LOG MONITORING

Rationale

The following factors mean that the monitoring of logs must adhere to certain principles:

- proper normalisation and correlation of logs will help generate meaningful automated alerts;
- automated alerts in combination with regular monitoring will facilitate the timely detection of security incidents; and
- clear guidance on incident response will ensure that all detected security incidents are investigated and handled correctly.

8.1. Log normalisation

(M = mandatory, R = recommended)

S/N	Requirement	Implementation
1.	The technology used at the logging facility **should** normalise all incoming log data, where technically possible, so that events can be efficiently correlated.	R
2.	A dedicated log repository **shall** be used to analyse actively events occurring on the Commission's systems and network.	M

8.2. Establishing a baseline

(M = mandatory, R = recommended)

S/N	Requirement	Implementation
1.	In order to detect deviations from normal system and network behaviour, the European Commission **shall** define it, taking account *inter alia* of the standard on network security. Said deviations will generate alerts.	M
2.	The baseline for normal behaviour **shall** be constantly updated in line with modifications to the European Commission's infrastructure, system configuration changes, the outcome of risk assessments and any other relevant information.	M

8.3. Using additional data sources

(M = mandatory, R = recommended)

S/N	Requirement	Implementation
1.	To improve understanding of events in the European Commission's environment, the log information in the central logging facility **shall** be combined with additional data from, *inter alia*: a. asset inventory list; b. the network model for each monitored information system or service, including the IP addressing plan, application and service network flows, and NAT policies; c. reporting from third-party applications for which no direct log files can be gathered; d. results of vulnerability scans and risk assessments; e. threat intelligence; and f. status of the anti-virus and the virus definitions database.	M

8.4. Scenarios for security event monitoring

(M = mandatory, R = recommended)

S/N	Requirement	Implementation
1.	The scenarios to be monitored **shall** include: a. logins after office hours or during off hours; b. multiple login failures followed by successful login for the same account; c. modification or deletion of log files; d. changes to the logging policy settings; e. anomalies detected in log files (e.g. missing line numbers, wrong file format); f. security configuration changes; g. unusual file transfers (as regards size, frequency and timeframe); h. internal systems with highest count of alerts in NIDS, NIPS or WAF; i. generation of abnormally high volumes of logs (log volume trends); j. deviations in database usage; k. discrepancies between the display name and the smtp address in the sender field of e-mails; and l. changes in the threat landscape.	M
2.	Based on the scenarios selected under 7.4.1, information from the available log files stored at the central logging facility **shall** be selected to provide a basis for monitoring these activities.	M

S/N	Requirement	Implementation
3.	The SOC **shall** review reporting and alerts based on the monitored activities.	M

8.5. Response to incidents

(M = mandatory, R = recommended)

S/N	Requirement	Implementation
1.	Alerts **should** be acknowledged within 60 minutes of the automated alert being generated.	R
2.	Automated alerts **shall** be investigated and, where a potential IT security incident is identified, give rise to an IT security incident ticket and be categorised and handled in accordance with Commission incident management procedures.	M

8.6. Reporting

(M = mandatory, R = recommended)

S/N	Requirement	Implementation
1.	Monthly management reporting **shall** indicate: a. alert response times (average, mean, min. and max. response time); b. the time taken to resolve each issue (average, mean, min. and max. response time); and c. an overview of the 10 most frequent alerts.	M
2.	A monthly alert overview **shall** be generated and sent to the threat intelligence team, so that they can fine-tune their activities.	M

9. FINAL PROVISION

This standard shall enter into force on the day following the date of its adoption. In accordance with Commission Decision (EU, Euratom) 2017/46 and Commission Decision (EU, Euratom) 2017/8841 (its Implementing Rules), and in particular Article 12, the logging and monitoring standard relating to Commission Decision C(2006) 3602 is repealed.