REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Nr. 1016 Prot   Tiranë më 07. 11 .2024

URDHËR

Nr. 408 datë. 07. 11. 2024

PËR
MIRATIMIN E RREGULLORES "PËR MËNYRAT DHE AFATET E RUAJTJES SË LOG-EVE TË INCIDENTEVE TË SIGURISË KIBERNETIKE"

Në zbatim të nenit 13 shkronja "f", nenit 16 shkronja "ç", si dhe nenit 17 shkronja "dh" të ligjit nr. 25/2024 "Për sigurinë kibernetike",

URDHËROJ:

1. Miratimin e rregullores "Për mënyrat dhe afatet e ruajtjes së log-eve të incidenteve të sigurisë kibernetike" sipas tekstit që i bashkëlidhet këtij urdhri dhe është pjesë përbërëse e tij.
2. Për zbatimin e këtij urdhri ngarkohen Autoriteti Kombëtar për Sigurinë Kibernetike, CSIRT-et sektoriale, si dhe CSIRT-et pranë operatorëve të infrastrukturave të informacionit.
3. Ky urdhër hyn në fuqi menjëherë.

DREJTORI I PËRGJITHSHËM

IGLI TAFA

REPUBLIKA E SHQIPËRISË - KËSHILLI I MINISTRAVE
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

REPUBLIKA E SHQIPËRISË

NATIONAL AUTHORITY FOR CYBER SECURITY

REGULATION

ON THE METHODS AND DEADLINES FOR STORING CYBERSECURITY INCIDENT LOGS

CONTENTS

pag

e

CHAPTER I

GENERAL PROVISIONS

Article 1

Object and purpose

The subject matter of this regulation is the determination of procedures and deadlines for the retention of logs of cyber security incidents identified by the CSIRT at the operator and reported to the sectoral and the National CSIRT, with the aim of ensuring their secure storage, protection, access, and destruction..

Article 2

Legal basis

This regulation is drafted pursuant to Article 13 letter "f", Article 16 letter "ç", as well as Article 17 letter "dh" of Law no. 25/2024 "Për sigurinë kibernetike".

Article 3

Scope of application

This regulation is mandatory to be implemented by the CSIRT at the operator, the sectoral CSIRT, and the National CSIRT regarding the logs of cybersecurity incidents that are created, stored, accessed, and destroyed in digital and physical space.

Article 4

Roles and responsibilities

The roles and responsibilities of the National CSIRT, sectoral CSIRT, and the operator's CSIRT in maintaining the logs of cybersecurity incidents in implementation of this regulation are as follows:

1. The National CSIRT, as the Computer Security Incident Response Team, secures the incident logs from the reports of the CSIRT submitted to the operator and, in this context, has the obligation to retain these logs in accordance with the procedures and deadlines specified in this regulation.

2. The Sectoral CSIRT, as the Computer Security Incident Response Team for the relevant sector, ensures the logs of incidents from the reports of the CSIRT with the operator, and in this context has the obligation to store these logs according to the manner and deadlines specified in this regulation.
3. The CSIRT at the operator, as the Cybersecurity Incident Response Team, ensures the logs of incidents from the detection of cybersecurity incidents at information infrastructures and, in this context, has the obligation to retain these logs according to the manner and timeframes specified in this regulation.

Article 5

Definitions

The terms used in this regulation have the same meaning as the terms defined in Law No. 25/2024 "Për sigurinë kibernetike", while the following terms have these meanings:

1. "CIA" refers to confidentiality, integrity, and availability, based on the principle of protecting information and sensitive data from potential threats and risks of cyber security.
2. "AAA" refers to authentication, authorization, and accountability to ensure full access control and monitoring of activities in information systems.
3. "RBAC" refers to the method for managing access to systems using roles, where each role is a group of privileges that can be assigned to users in the system.

CHAPTER II

METHODS, DEADLINES AND ACCESS TO THE STORAGE OF LOGS

Article 6

Methods of storing incident logs

The logs of cybersecurity incidents are stored in digital and physical space.

1. The retention of logs in digital space must be carried out in accordance with the following provisions:
   a) Incident logs must be retained by the CSIRT at the operator, the Sectoral CSIRT, and the National CSIRT, based on the CIA principle. Furthermore, the logs may also be retained in a **central system** managed by the National CSIRT.
   b) Access to the incident log storage system must be restricted only to authorized personnel according to the AAA principle.

   c) "Backups" of the logs must be stored in an isolated and physically separate location according to internationally recognized standards.

2. The storage of incident logs in the physical space must be carried out in accordance with the following provisions:
   a) The storage of incident logs in the physical space is carried out in a closed area, with controlled access.
   b) Access to the physical premises must be restricted to authorised personnel only.

Article 7

Protection of incident logs

To ensure the protection of incident logs, all of the following processes are applied:

1. **Encryption:** All incident logs stored in the digital space must be encrypted using strong encryption algorithms to ensure the confidentiality and integrity of the data both in storage and during transmission.
2. **Access control:** Role-based access control (RBAC) should be applied to incident logs to ensure that only authorized personnel can access them.
3. **Monitoring**: The log retention system must be continuously monitored, at least twice a year, to identify any unauthorized access to them.
4. **Availability**: To ensure the security and accessibility of logs of cybersecurity incidents, so that they can be used when needed, regardless of possible risks or incidents, as one of the main components of information security.
5. **Immunity of Systems and Applications:** CSIRTs must ensure the integrity of all processes of the systems and applications that generate logs.
6. **Tracing**: The log tracing process must ensure the collection, storage, and analysis of the information recorded in the logs to monitor the activities of systems and users, in order for these activities to be traceable and auditable accurately and effectively, enabling identification, analysis, prevention, and improvement in response to cybersecurity incidents.
7. **Incident handling in the event of a breach of log retention**: In the event of a breach of the security, integrity, and confidentiality of incident logs, immediate measures must be taken in accordance with the provisions of the applicable regulation on the management of cybersecurity incidents.

Article 8
Access to the log storage areas

1. Every request to access the digital and physical space where the logs of cybersecurity incidents are stored must be officially documented and approved by the head of the CSIRT or a person authorized by him.
2. All accesses to the log incident storage areas must be recorded, including the identity of the user, the time of access, the user’s permissions, and the nature of the access.
3. Personnel who enter the log incident retention areas have the obligation to implement the principle of confidentiality.

Article 9

The retention periods of incident logs

The retention period of logs by CSIRTs in digital space and physical space in implementation of this regulation is as follows:

1. Incident logs containing personal data are stored by the CSIRT at the operator in accordance with the timeframes specified by the applicable legislation on personal data.
   Incident logs that do not contain personal data are retained by the CSIRT at the operator for a period ranging from 1 (one) year to 3 (three) years, depending on the risk and operational requirements.
2. Incident logs containing personal data are stored by the sectoral CSIRT in accordance with the deadlines specified in the applicable legislation on personal data.
   Incident logs that do not contain personal data are retained by the sectoral CSIRT for a period from 1 (one) year to 3 (three) years, depending on the risk and operational requirements.
3. Incident logs containing personal data are stored by the National CSIRT in accordance with the provisions of the applicable legislation on personal data.
   Incident logs that do not contain personal data are retained by the National CSIRT for a period from 1 (one) year up to 3 (three) years, depending on the risk and operational requirements.

CHAPTER III

DESTRUCTION OF INCIDENT LOGS

Article 10

Destruction of incident logs

1. After the expiration of the deadlines specified in Article 9 of this regulation, CSIRTs are obliged to destroy these logs.
2. Logs stored in the digital space must be destroyed using secure erasure methods, such as cryptographic erasure or overwriting, ensuring that they cannot be recovered.
3. Logs stored in physical space must be shredded or incinerated to ensure their complete destruction.
4. The destruction of incident logs must be documented by means of a minutes, in which the date, method, and persons involved in the destruction process are identified/recorded.

CHAPTER IV

COMPLIANCE AND TRAINING

Article 11

Compliance

1. CSIRTs must carry out regular compliance checks to ensure the fulfilment of the obligations set out in this regulation.
2. All actions related to the storage, access, and destruction of incident logs must be auditable, as well as documented by the CSIRTs.

Article 12.

Training of personnel

CSIRTs must conduct regular training programs to ensure that all personnel involved in managing the storage of incident logs are aware of their responsibilities and the procedures described in this regulation.