REPUBLIC OF ALBANIA
NATIONAL AUTHORITY ON ELECTRONIC CERTIFICATION AND CYBER SECURITY

Regulation on Categorising Cyber Incident, the format and elements of the report

Approved by Order no. 62, dated 10.09.2018, of the General Director
of the National Authority on Electronic Certification and
and Cyber Security (NAECCS)

Contents

Introduction..2

Purpose...2

Categories of Cyber Incidents...2

Cyber incident escalation procedure...8

Cyber incident reporting form..10

Incidents that do not need to be reported...12

Introduction

Effective cyber security management involves a combination of cyber incident prevention, detection and incident response. In order to achieve a high level of security, a critical or important information infrastructure must be able to respond to incidents and have appropriate procedures adopted in the event that an incident that compromises information security occurs.

For an efficient solution of potential cyber security incidents, it is necessary to categorize cyber incidents, as well as define the incident escalation procedure from identification, treatment to its solution.

This regulation was drafted on the basis of Law No. 2 dated 26.01.2017 on "Cyber Security", Article 11 point 2.

Purpose

The purpose of drafting this regulation is to define the categories of cyber security incidents, the format and elements of the report as well as the cyber incident escalation procedure.

Categories of Cyber Incidents

A cyber security incident is a cyber security event, during which a violation of the security of services or information systems and communication networks is caused and brings a real negative effect.

Once an incident is reported, it must be handled efficiently and quickly until it is resolved. Categorizing cyber incidents helps to plan actions for incident response and helps parties meet the reporting timeline, depending on the critical or important information infrastructure the operator owns.

Category	Definition	Description	Reporting timeline	
			Critical system	Important system
1	Compromised information	• Alteration or disclosure of sensitive information • Attack on information that is considered intellectual property	Within 4 hours after determinig the incident has occurred.	Within 24 hours after determinig the incident has occurred.
2	Compromised Asset	• Compromised host (root, Trojan, rootkit) • compromised network devices, applications, and user accounts. • Hosts infected with malware where the attacker actively controls the host.	Within 4 hours after determinig the incident has occurred.	Within 24 hours after determinig the incident has occurred.
3	Unauthorised Access	• An individual (internal or external) has logical or physical access without permission:	Within 4 hours after determinig the incident has occurred.	Within 24 hours after determinig the incident has occurred.

		- in a national or local network - in a system - in an application - to the data - or other sources in an unauthorized manner		
4	Malicious Code	• Successful installation of malicious software such as: - virus, - worm, - Trojan horse, - or other malicious codes that infect an operating system or application. • Institutions are not required to report malicious code that has been detected and isolated by antivirus.	• Within 4 hours after determinig the incident has occurred if it has been distributed throughout the institution. • Within 4 days hours after determinig the incident has occurred if not distributed	• Within 24 hours after determinig the incident has occurred if distributed throughout the institution. • Within 24 days hours after determinig the incident has occurred if not distributed.
5	Intrusions against networks	• Attack that impairs the normal functionality of: - networks	• Within 4 hours of detection if the attack is ongoing	• Within 24 hours of discovering whether the attack

		- systems - applications, depleting resources through: - DDoS - Web defacement - Brute force attacks	and the institution is unable to stop it.	is ongoing and the institution is unable to stop it.
6	Phishing or Social Engineering	• The use of technology to learn from the employees of the institution important information such as: -username - passwords - other information sensitive etc	• Within 4 hours after determinig the incident has occurred.	• Within 24 hours after determinig the incident has occurred.
7	Unlawful activity	• Frauds computer • Pornography with him JUVENILE • Incidents computer with criminal nature, the solution of which may involve other organs law enforcement, investigations global etc.	• Within 4 hours after determinig the incident has occurred.	• Within 24 hours after determinig the incident has occurred.

8	Scans/Probes/ Attempted Access	- This category includes any activity that accesses or identifies: - a computer of the institution, - open ports, - protocols, - services, or any combination to use later. - This activity directly results in a compromise or denial of service.	- Within 4 hours after determinig the incident has occurred.	- Within 24 weeks after determinig the incident has occurred.
9	Policy Violations	- Intentional policy violations such as: - Inappropriate use of institution assets such as computer, network, or application. - Unauthorized escalation of privileges or deliberate attempt to subvert access controls.	- Within 4 hours after determinig the incident has occurred.	- Within 24 weeks after determinig the incident has occurred.
10	Theft/loss of assets	- Theft or loss of information or equipment	- Within 4 hours after determinig the	- Within 24 hours after determinig the

		that can be used to process or store sensitive information	incident has occurred.	incident has occurred.
11	Unauthorised release of or disclosure of information	• Extracting or publishing information in an unauthorized manner	• Within 1 hour after determinig the incident has occurred.	• Within 2 hours after determinig the incident has occurred.

Cyber incident escalation procedure

The cyber incident escalation procedure defines the steps that are followed from the moment the incident is reported by the sectoral CSRT to NAECCS through the cyber incident reporting form, until the resolution or closure of the incident.

The parties involved in the escalated procedure should be identified depending on the type and importance of the incident, taking into account the affected information infrastructure.

An incident may initially involve only internal staff. Senior managers of the operator that owns the infrastructure may be notified at a later stage of incident handling. If the incident cannot be resolved, the support of other parties should be sought, such as: the company that has the maintenance of the system/network, NAECCS, and if it is estimated that the incident constitutes a criminal offense, the Anti-Cybercrime Sector in the State Police should be notified. **At the moment the incident is reported to the Cyber Crime Sector in the State Police, NAECCS stops handling the reported incident.**

In any case, regardless of how the incident is resolved, the operator must report the incident to NAECCS by completing the "Cyber incident reporting form".

Data on reported incidents will be collected by NAECCS in an electronic register with the aim of:

a) Taking measures to prevent similar incidents in the future by analyzing the incident.

b) The recording of the incidents that occurred for keeping statistics, which provide a general overview of the type, size and frequency of cyber incidents.

Each system/network should have its own escalation procedure and points of contact that meet their specific operational needs. Different people may be notified at different stages, depending on the damage to the system, or the sensitivity of the data affected.

Points of contact to include, but not be limited to, are:

- Internal

  a) Technical and operational support staff;
  b) System manager and/or superior;
  c) Safety officer/CSIRT of the operator
  d) Coordinator for information, preparation and distribution through the media information.

- External

  a) The company that maintains the system, software developers, security consultants, etc.;
  b) Service Providers (eg Internet Service Providers (ISPs), contracting parties, etc.);
  c) AKCESK;
  d) Representative from the Commissioner for the Right to Information and Protection of Personal Data (IDP);
  e) Representatives from the Cyber Crime Sector at the State Police;
  f) Subjects and affected individuals

Cyber incident reporting form			
Section 1: Reporter's contact details			
Name/Surname:		Work position:	
Institution:		E-mail:	
Tel:		Cel:	
Infrastructure data affected by the attack			
System/Network Name:			
Type of information infrastructure: □ Critical			
□ Important			
Type of assistance you require from NAECCS			
□ Report only	□ Treatment	□ Recommendations	
Section 2: Incident details			
Identification of the incident			
□ Device alarm	□ Analysis of logs	□ Help desk	
□ Notice from the user	□ Notice from Endpoint Security Software		
□ Other:			
The Current Status of the Incident			
□ Is happeninng	□ Under control	□ Has happened	
Category pf the incident			
□ Compromised information	□ Compromised asset	□ Unauthorised access	□ Malicious code

□ Intrustions against network	□ Theft or Lost	□ Scans/Probes/Attempted Access	
□ Phishing or Social Engineering	□ Policy violations	□ Theft/loss of assets	
□ Unauthorised release of or disclosure of information	□ Other		
Incident data			
Source IP/Port:		Destination IP/Port:	
Was the data involved in the incident encrypted:	□ Yes □ No		
Duration of the incident			
From date/hour:		To date/hour:	
Incident Impact			
The number of affected users:			
Time the system is out of service:			
System damage:			
Financial loss:			
Whether or not there is data loss:			
Please include 5-10 lines of time stamped logs in plain ASCII			

Please give a brief description of the incident and the consequences

The cyber incident reporting form should be send to the e-mail address: info@cesk.gov.al.

Incidents that do not need to be reported

- A malware or virus on an employee's device that can be easily repaired, eg: (*single instance of a user device with a virus that is automatically detected and easily cleaned*)
- Short-term interruptions in non-critical services, eg: (*equipment having an unplanned outage which was easily restored in a short time*)
- Single cases of standard spam e-mails that do not contain malicious links or attachments, eg: (*marketing or advertising but no clickable links or attachments*)
- Employees violating institution-specific policies or guidelines for Internet use, eg: (*single users browsing inappropriate, but not illegal or malicious, sites during working hours*)
- Exploited vulnerability in non-critical information systems, services or networks, eg: (*weakness on a user's desktop which has not been exploited*)