Manual for Incident Reporting by the Constituents

Version 1.0 - 23.03.2018

Document classification: PUBLIC / TLP WHITE

Contents

1. Introduction

The response to a reported incident shall depend on the quality of information reported by the constituent, framework of reporting, and the capacity of the authority, institution or legal persons, responsible for resolving the issues that have occurred due to the reported incident. This Manual defines the manner and procedure of reporting the incident and defines the general terms used in the communication between MKD-CIRT and the constituents.

1.1 Objective

The objective of this Manual is to help any constituent report an incident to MKD-CIRT within the timeframe requested.

1.2 Scope

This Manual shall pertain to the MKD-CIRT Team and its constituents.

1.3 References

[1] Policy on information classification of MKD-CIRT

[2] Policy on information disclosure

1.4 Abbreviations

Abbreviation	**Description**
MKD-CIRT	National Centre for Computer Incident Response in the Republic of Macedonia
CAT	Incident category
DNS	Domain Name System
IP	Internet protocol

Table 1: Abbreviations and description

2. Definitions

2.1 Event

Event is the occurrence or change of particular group of circumstances, and it may:

- be one or several occurrences and may have several causes
- consist of something that is not occurring
- be considered as "incident" or "accident”.

Information Security Event

Information security event is an occurrence on the system, services or network, indicating a possible breach of the information security policy or violation of the safeguards, or a previously unknown situation that may be relevant to the security.

Information Security Incident

Information Security Incident (hereinafter: incident) shall mean single or series of undesired or unexpected information security events, which may compromise the operations of a single organisation or individual, and represents threat to information security.

2.4 Critical System

Critical system shall mean system comprised of applications, data, or other resources that are essential for the survival of an organization. In case a critical system is not operational or its operations have been interrupted, the main operations of the organization are significantly disrupted.

2.5 Non-critical system

Non-critical system shall mean system comprised of applications, data or other resources which, if compromised, have no major impact on the performance of the main operations of the organization.

3. Guidelines for incident reporting

The Incident Report should include a description of the incident or event, using the appropriate taxonomy, and as many of the following information:

- Protection of information submitted
  - Protection level (Strictly Confidential, Confidential or Public)
- Contact Information
  - Name and surname of person in charge
  - E-mail address
  - Telephone number
- Details of the incident
  - Date and time of detection
  - Time zone
  - Level of impact on the organization (Critical, High, Low, No Impact, or Unknown)
  - Category incident (one between CAT 1 and CAT 10 as per Table 2)
  - Current status (On-going, Incident is under control (localized), Incident has occurred previously, and Unknown)
  - Number of affected systems (estimate)
  - Features (description) of the incident
- System details
  - Name and address (Host / IP)
  - System function (e.g.: DNS system, Web server, E-mail server, etc.).
  - Tracking the incident report (Initial Report to MKD-CIRT, Continuation of a previous report)

The constituent should use this model when reporting an incident to MKD-CIRT. Depending on the incident criticality, it is not always possible to gather all the necessary information before reporting the incident. In this case, the constituent should submit the incident report and continue with additional submissions of information as soon as such information become available.

The Incident Report Form for the constituents is available on the web-site of MKD-CIRT (https://mkd-cirt.mk). Once the constituent fills out the form, it should send it within the required timeframe (according to Table 2) at the following e-mail address: soc@mkd-cirt.mk or via fax at **+389 2 3224 611** (not deemed as safe incident report). When sending the report via e-mail, it must be electronically signed by the constituent and encrypted with the public key of MKD-CIRT, available on the web-site https://mkd-cirt.mk.

Actions undertaken by MKD-CIRT to prevent the spreading of the incident shall be limited to the minimum required ones (without installations of systems and software at the constituent side), in order to preserve the evidence and preserve the investigative capacity of MKD-CIRT.

All other issues related to the operations of MKD-CIRT, and not pertaining to the incident reporting, may be sent by the constituents at the following e-mail info@mkd-cirt.mk or phoned in during working hours on the following telephone number **+389 2 3289 200**.

4. Timeframe for incident reporting

The timeframe within which the constituent should report the incident is defined in Table 2 of this Manual. Upon exceeding this timeframe, MKD-CIRT shall not be responsible for the efficient resolution of the reported incident.

5. Service level

Upon registration of the incident by the MKD-CIRT, the system automatically e-mails a notification message to the applicant (constituent). This message informs the applicant:

- that the incident report will be reviewed by MKD-CIRT
- of the report number to be used in communication with the MKD-CIRT with regards to this reported incident

Upon creating the incident report, MKD-CIRT shall commence the incident identification stage (categorising the incident and assigning its priority). This stage is followed by the incident response stage, which is an integral part of the incident resolution.

The priority levels of the incident and the timeframes for **initiating** the incident response stage, which includes the prevention of incident spreading, threat eradication, as well as recovery of the targeted information system, are given in Table 1 of this Manual.

Levels	**Maximum timeframe for initiating the incident response stage**
Priority 1 Very high	24h after incident registration
Priority 2 High	16h after incident registration
Priority 3 Medium	8h after incident registration
Priority 4 Low	4h after incident registration

Table 1: Priority levels

6. Incident categorisation

MKD-CIRT and its constituents have to adopt common terms and relations thereof for the purpose of having clear information about the incidents and events (each observed occurrence in a network or a system) at any of the constituents.

Table 2 lists the concepts and the categorisation descriptions of computer security incidents.

How to use Table 2: It starts by reading from top to bottom and selecting the first category corresponding to the incident reported.

Category	**Designation**	**Description**	**Timeframe for notification**	
			Critical System	Non-Critical System
CAT 1	Compromised information	Successful destruction, corruption, or disclosure of sensitive information or intellectual property.	Within one (1) hour of discovery/ detection.	Within four (4) hours of discovery/ detection.
CAT 2	Compromised asset	Compromised device (system account, trojan, rootkit), network device, application, user account. This includes devices infected by malware, where the attacker is actively controlling the device.	Within one (1) hour of discovery/ detection.	Within one (1) hour of discovery/ detection.
CAT 3	Unauthorized access	In this category, an individual (employee or external party) has gained logical or physical access without permission to a national or local network, system, application, data or other resources.	Within one (1) hour of discovery/ detection.	Within four (4) hours of discovery/ detection.
CAT 4	Malicious code	Successful installation of malware (e.g. virus, worm, trojan or other type of malicious code) that has infected the operating system or a specific application. The constituents are not obliged to report the malicious logic of the antivirus software which has successfully quarantined the malware.	Within one (1) hour of discovery/ detection if it has been widespread across the organization, otherwise one (1) day.	Within four (4) hours of discovery/ detection if it has been widespread across the organization, otherwise one (1) day.

CAT 5	(Distributed) Denial of Service	Attack that successfully prevents or disrupts the normal operation of networks, systems, or applications by exhausting/flooding their resources. This activity involves the role of a victim or participant in the DoS.	Within two (2) hours of discovery/ detection if the attack is still successfully on-going and the organization is not able to successfully mitigate this action.	Within four (4) hours of discovery/ detection if the attack is still successfully on-going and the organization is not able to successfully mitigate this action.
CAT 6	Theft or loss	Theft or loss of sensitive equipment (laptop, hard drive, media and other equipment) of the organization.	Within one (1) day of discovery/ detection.	Within one (1) week of discovery/ detection.
CAT 7	Phishing	Use of fake computer network technology to entice users in the organization to reveal important information, such as details and authorisations for bank accounts of customers through deceptive messages received via e-mail or fraudulent web-sites	Within four (4) hours of discovery/ detection.	Within one (1) day of discovery/ detection.
CAT 8	Unlawful activities	Fraud / Human Security / Child pornography. Computer incidents of a criminal nature, often including the executive branch of the government, international investigations or prevention of loss.	Within six (6) hours of discovery/ detection.	Within one (1) day of discovery/ detection.
CAT 9	Scans / probes / Access attempts	This category includes any activity that seeks access or identification of the organization's computers, open ports, protocols, services, or any combination thereof, for later exploitation. This activity does not directly result in a compromise or denial of service.	Within one (1) hour of discovery/ detection.	Within two (2) weeks of discovery/ detection.

CAT 10	Policy violations	Intentional violations of the information security policy, such as: improper use of corporate assets, such as computers, networks, or applications. Unauthorized increase of privileges or deliberate attempt to bypass access controls.	Within six (6) hours of discovery/ detection.	Within one (1) week of discovery/ detection.

Table 2: Categories of information security incidents

7. Policy on information disclosure

All information intended for MKD-CIRT shall be processed in accordance with the Policy on information disclosure of MKD-CIRT, published on the web-site of MKD-CIRT (https://mkd-cirt.mk).

8. Appendix

The document Incident Reporting Form for MKD-CIRT (.docx) is enclosed to this Manual.