Упатство за пријава на инциденти од конституентите

Верзија 1.0 - 14.04.2016

Класификација на документот: JABHO / TLP WHITE

MKD-CIRT
РЕПУБЛИКА МАКЕДОНИЈА
АГЕНЦИЈА ЗА ЕЛЕКТРОНСКИ КОМУНИКАЦИИ
НАЦИОНАЛЕН ЦЕНТАР ЗА ОДГОВОР
НА КОМПЈУТЕРСКИ ИНЦИДЕНТИ

Содржина

1. Вовед

Одговорот на пријавен инцидент зависи од квалитетот на информациите пријавени од конституентот, од временската рамка за пријавување и од капацитетот на органот, институцијата или правното лице, кои се одговорни за решавање на проблемите настанати од пријавениот инцидент. Ова упатство ги дефинира начинот и постапката на пријавување на инцидент и ги дефинира општите термини што се користат во комуникацијата меѓу MKD-CIRT и конституентите.

1.1 Цел

Целта на ова упатство е да му помогне на конституентот да го пријави инцидентот до MKD-CIRT во бараната временска рамка.

1.2 Опсег

Ова упатство се однесува на тимот на MKD-CIRT и неговите конституенти.

1.3 Референци

[1] Политика за класификација на информации на MKD-CIRT
[2] Политика за откривање на информации

1.4 Кратенки

Кратенка	**Опис**
MKD-CIRT	Национален центар за одговор на компјутерски инциденти во Република Македонија
КАТ	Категорија на инцидент
DNS	Domain Name System - Систем за имиња на домени
IP	Интернет протокол

Табела 1: Кратенки и опис

2. Дефиниции

2.1 Настан

Настан е случување или промена на одредена група околности, и истиот:

- може да биде една или повеќе појави и може да има неколку причини.
- може да се состои од нешто што не се случува.
- може да се смета како "инцидент" или "несреќа".

2.2 Информациски безбедносен настан

Информациски безбедносен настан е појава на системот, на услугите или мрежата што укажува на можно прекршување на политиката за безбедност на информации или прекршување на заштитни мерки, или пак претходно непозната ситуација која може да биде релевантна за безбедноста.

2.3 Информациски безбедносен инцидент

Информациски безбедносен инцидент (во понатамошниот текст: инцидент) е еден или серија на несакани или неочекувани информациски безбедносни настани, кои може да ја компромитираат работата на една организација или индивидуа и претставуваат закана за безбедноста на информациите.

2.4 Критичен систем

Критичен систем е систем, составен од апликации, податоци или други ресурси што се од суштинско значење за опстанокот на една организација. Во случај кога критичниот систем не работи или е прекинат во работата, основните операции на организацијата се значително нарушени.

2.5 Некритичен систем

Некритичен систем е систем, составен од апликации, податоци или други ресурси кој доколку е компромитиран нема големо влијание врз извршувањето на основните операции на организацијата.

3. Упатство за пријава на инцидент

Пријавата за инцидент треба да вклучи опис на инцидентот или настанот, користејќи ја соодветната таксономија, и што е можно повеќе од следните информации:

- Заштита на доставената информација
  - Ниво на заштита (Строго доверливо, Доверливо или Јавно)
- Информации за контакт
  - Име и презиме на одговорно лице
  - Ареса за електронска пошта
  - Телефонски број
- Детали за инцидентот
  - Датум и време на откривање
  - Временска зона
  - Ниво на влијание врз организацијата (Критично, Високо, Ниско, Нема влијание или Непознато)
  - Категорија на инцидент (една од КАТ 1 до КАТ 10 согласно Табела 2)
  - Моментална состојба (Тековно се случува, Инцидентот е под контрола (локализиран), Инцидентот се случи претходно и Непознато)
  - Број на засегнати системи (проценка)
  - Карактеристики (опис) на инцидентот
- Детали за системот
  - Име и адреса (Host / IP)
  - Функција на системот (пр: DNS систем, Веб сервер, Сервер за електронска пошта и сл.)
  - Следење на пријавата за инцидент (Првична пријава до MKD-CIRT, Продолжение на претходна пријава)

Конституентот треба да го користи овој модел при пријава на инцидент до MKD-CIRT. Зависно од критичноста на инцидентот, не е секогаш можно да се приберат сите потребни информации пред пријавување на инцидентот. Во ваков случај, конституентот треба да ја достави пријавата за инцидент и да продолжи со дополнителни достави на информации како што информациите ќе станат достапни.

Формуларот за пријава на инцидент од страна на конституенти е достапен на веб-страницата на MKD-CIRT (https://mkd-cirt.mk). Откако конституентот ќе го пополни формуларот, истиот треба да го испрати во бараната временска рамка (согласно табела 2) на адреса за електронска пошта: soc@mkd-cirt.mk или по факс на број +389 2 3224 611 (не безбедна пријава на инцидент). При испраќање на Пријавата по електронска пошта, истата задолжително треба да е електронски потпишана од страна на конституентот и шифрирана со јавниот клуч на MKD-CIRT што е достапен на веб-страницата https://mkd-cirt.mk.

Преземените активности од страна на MKD-CIRT за спречување на проширување на инцидентот ќе се ограничат на минимално потребни (без инсталации на системи и софтвери кај конституентот), заради зачувување на доказите и зачувување на истражните капацитети на MKD-CIRT.

Сите други прашања кои се од областа на работењето на MKD-CIRT, а не се однесуваат за пријава на инцидент конституентот може да ги испрати на адреса за електронска пошта info@mkd-cirt.mk или да се јави во работно време на телефонски број +389 2 3091 232.

4. Временска рамка за пријава на инцидент

Временската рамка во која конституентот треба да го пријави инцидентот е дефинирана во табела 2 на ова Упатство. По надминување на оваа временска рамка MKD-CIRT не одговара за ефикасно решавање на пријавениот инцидент.

5. Ниво на услуга

По регистрација на инцидентот од страна на MKD-CIRT, системот автоматски испраќа порака за известување по електронска пошта до пријавувачот (конституентот). Оваа порака го информира пријавувачот:

- дека пријавата за инцидент ќе биде разгледана од страна на MKD-CIRT
- за бројот на пријава што ќе се користи во комуникацијата со MKD-CIRT за овој пријавен инцидент

По креирање на пријавата за инцидентот, MKD-CIRT ја почнува фазата на идентификација на инцидентот (категоризација на инцидент и одредување на приоритет). По оваа фаза следи фаза за одговор на инцидент која е составен дел од решавање на инцидентот.

Нивоата на приоритет на инцидентот и временските рамки **за отпочнување** на фаза за одговор на инцидент што опфаќа спречување на проширување на инцидентот, искоренување на заканите, како и закрепнување на целниот информациски систем, се дадени во Табела 1 на ова Упатство.

Нивоа	**Максимална временска рамка за отпочнување на фазата за одговор на инцидент**
Приоритет 1 Многу високо	4h по регистрација на инцидент
Приоритет 2 Високо	8h по регистрација на инцидент
Приоритет 3 Средно	16h по регистрација на инцидент
Приоритет 4 Ниско	24h по регистрација на инцидент

Табела 1: Нивоа на приоритет

6. Категоризација на инцидент

MKD-CIRT и неговите конституенти потребно е да усвојат заеднички термини и релации помеѓу нив за јасно информирање за инциденти и настани (секоја забележана појава во мрежа или систем) кај било кој конституент.

Во табела 2 се наведени концепти и описи за категоризација на компјутерски безбедносни инциденти.

Начин на користење на табела 2: Се започнува со читање од горе надолу и се избира првата категорија која одговара на инцидентот што се пријавува.

Категорија	Назив	Опис	Временска рамка за известување	
			Критичен систем	Не критичен систем
КАТ 1	Компромитирана информација	Успешно уништување, расипување, или откривање на чувствителни информации или интелектуална сопственост.	Во рок од еден (1) час од откривање/детекција.	Во рок од четири (4) часа од откривање/детекција.
КАТ 2	Компромитирано средство	Компромитиран уред (системска сметка, тројанец, rootkit), мрежен уред, апликација, корисничка сметка. Ова вклучува уреди инфицирани со штетен софтвер (malware) каде напаѓачот активно го контролира уредот.	Во рок од (1) час од откривање / детекција	Во рок од (1) час од откривање/детекција
КАТ 3	Неавторизиран пристап	Во оваа категорија поединец (вработен или надворешно лице) без дозвола се здобива со логички или физички пристап до национална или локална мрежа, систем, апликации, податоци или други ресурси.	Во рок од (1) час од откривање/детекција	Во рок од четири (4) часа од откривање/детекција
КАТ 4	Штетен (малициозен) код	Успешна инсталација на штетен (малициозен) софтвер (пр. Вирус, црв, тројанец или друг штетен код) што ги инфицира оперативниот систем или одредена апликација. Конституентите не се обврзани да известат за малициозната логика на софтверот за антивирус кој успешно го ставил во карантин штетниот софтвер.	Во рок од еден (1) час од откривање/детекција доколку има широка распространетост низ организацијата, во спротивно еден (1) ден.	Во рок од четири (4) часа од откривање/детекција доколку има широка распространетост низ организацијата, во спротивно еден (1) ден.

КАТ 5	(Distributed) Denial of Service / Дистрибуирано одбивање на услуга	Напад кој успешно го спречува или нарушува нормалното функционирање на мрежи, системи или апликации со исцрпување на ресурсите. Оваа активност вклучува улога на жртвата или учество во ДОУ.	Во рок од два (2) часа од откривање/детекција доколку нападот сеуште успешно се одвива и организацијата не е во можност успешно да ја ублажи активноста.	Во рок од четири (4) часа од откривање/детекција доколку нападот сеуште успешно се одвива и организацијата не е во можност успешно да ја ублажи активноста.
КАТ 6	Кражба или загуба	Кражба или загуба на чувствителната опрема (лаптоп, хард диск, медиуми и др. опрема) на организацијата.	Во рок од еден (1) ден од откривање/детекција.	Во рок од една (1) недела од откривање/детекција.
КАТ 7	Phishing	Употреба на лажна компјутерска мрежна технологија за да ги примами корисниците во организацијата да откријат важни информации, како што се детали и ингеренции за банкарски сметки на корисниците преку измамнички пораки добиени преку електронска пошта или лажни веб страни	Во рок од четири (4) часа од откривање/детекција	Во рок од еден (1) ден од откривање/детекција
КАТ 8	Незаконски активности	Измама /Човечка безбедност/ Детска порнографија. Компјутерски инциденти од криминална природа, најчесто со вклучена извршна власт, меѓународни истраги или превенција на губиток.	Во рок од шест (6) часа од откривање/детекција	Во рок од еден (1) ден од откривање/детекција
КАТ 9	Скенирања/Сонди /Обиди за пристап	Оваа категорија ја вклучува секоја активност која има за цел пристап или идентификација на организациски компјутери, отворени порти, протоколи, услуги, или било која комбинација од истите, за подоцнежна експлоатација. Оваа активност директно не резултира со	Во рок од еден (1) час од откривање/детекција	Во рок од две (2) недели од откривање/детекција

		компромитација или одбивањето на услуга. (Denial of service).		
КАТ 10	Повреди на политики	Намерни прекршувања на политиката за информациска безбедност како на пр: Несоодветна употреба на корпоративни средства како компјутер, мрежа, или апликација. Неовластена ескалација на привилегии или намерен обид за заобиколување на контроли за пристап.	Во рок од шест (6) часа од откривање/детекција	Во рок од една (1) недела од откривање/детекција

Табела 2: Категории на информациски безбедносни инциденти

7. Политика за откривање на информации

Сите информации наменети за MKD-CIRT се обработуваат согласно Политиката за откривање на информации на MKD-CIRT, објавена на веб-страницата на MKD-CIRT (https://mkd-cirt.mk).

8. Прилог

Документ во прилог на ова Упатство е Образец за пријава на инцидент во МКД-ЦИРТ (.docx).