Политика за откривање на информации

Верзија 1.0 – 16.03.2016

Класификација на документот: ЈАВНО / TLP WHITE

Содржина

1. Вовед

Обработката на осетливи информации е важен аспект во дневното работење на Националниот центар за одговор на компјутерски инциденти, понатаму MKD-CIRT. Осетлива информација може да се прими во MKD-CIRT преку достава на пријава на инцидент од страна на конституент или друга страна што учествува во процесот за управување со инцидент. Одржување на довербата во способноста на MKD-CIRT за заштита на осетливи информации е од суштинско значење за неговото работење. Правилата за откривање на информации опишани во овој документ имаат за цел да му помогнат на MKD-CIRT во одржување на високо ниво на доверба.

1.1. Цел

Оваа политика ги дефинира и опишува принципите кои MKD-CIRT ги следи во откривање, објава и споделување на информации и заедно со Политиката за класификација на информациите на MKD-CIRT е наменета за одржување на доверливоста на податоците што ги користи MKD-CIRT.

1.2. Опсег

Оваа политика ги опфаќа сите информациски средства, создадени, управувани, пренесувани или запишани од страна на MKD-CIRT.

1.3. Врски и референци

- Политика за класификација на информации
- Образец: Овластување за откривање на информации
- Образец: Договор за неоткривање на информации
- Закон за заштита на личните податоци
- Закон за електронските комуникации
  Законот за класифицирани информации

1.4. Кратенки

Кратенка	Опис
CERT	Computer Emergency Response Team
КИ	Критична Инфраструктура
CIRT	Computer Incident Response Team
CSIRT	Computer Security Incident Response Team
TLP	Traffic Light Protocol

2. Дефиниции

2.1. Информациска размена

Информациска размена е „размена на информации“ може да се врши лично, на пр. на состаноци со CSIRT тимови или на MKD-CIRT и неговите конституенти, или на состанок на кој учествуваат стручни лица за информациска безбедност; таа исто така може да биде и во форма на размена на пораки по електронска пошта или телефонски разговор.

2.2. Анонимизација

Анонимизација е бришење на идентификациските карактеристики на корисниците

3. Одговорност за управување со податоци

Сите членови на MKD-CIRT имаат обврска за заштита на доверливоста на податоците со кои работат, без оглед на формата или медиумот на кој податокот е запишан или преку кој се пренесува, согласно процедурите за работа на MKD-CIRT.

MKD-CIRT е одговорен за имплементација на соодветни процедурални, физички и технички контроли за пристап, користење, пренос или депонирање на податоците што се во сопственост на или ги користи MKD-CIRT во согласност со оваа политика.

Со цел да се избегне каква било протекување на осетливи информации, членовите на MKD-CIRT ќе откриваат информации само ако е неопходно и во согласност со следниве правила.

4. Откривање на информации

4.1. Заштита на информации

При размена на информации MKD-CIRT го користи принципот „потребно е да знае“ (need-to-know): Информацијата што не е јавна НЕ СМЕЕ јавно да се споделува, и МОРА да се сподели САМО со тие субјекти што треба да ја знаат.

Информацијата ќе се открива и споделува во согласност со оригиналното ниво на доверливост.

MKD-CIRT ја почитува доделената класификација на информацијата одредена од страна на изворот што ја доставил информацијата до MKD-CIRT во согласност со процедурите за внатрешно работење на MKD-CIRT.

Откривање и објава на осетливи информации ќе се врши САМО АКО Е ПОТРЕБНО за решавање на инцидентот. Во точка 3.3. – Анонимизација се наведени принципите на MKD-CIRT за откривање на информации од овој вид.

MKD-CIRT често соработува со повеќе групи вклучувајќи други CSIRT тимови и други засегнати страни, производители и добавувачи, извршни органи на власта и други. Откривањето на информации на овие групи ќе се врши на поединечна основа и сразмерно со ризикот од откривање на информацијата. MKD-CIRT го задржува правото пред откривање на информација да побара потпишување на Договор за неоткривање на информации.

Пред да се изврши размена на доверливи информации со други партнери, често други CSIRT тимови, кои се вклучени во истрагата за инцидентот по компјутерска безбедност, се потврдува чесноста на овие страни.

При комуникација со други CSIRT тимови и трети страни, MKD-CIRT ќе осигура дека информацијата што се прави достапна за други:

- е потпишана за да се обезбеди неотповикливост, и
- е шифрирана за заштита на доверливоста, секогаш кога е потребно во согласност со оваа политика

4.2. Заштита на лични податоци и правни аспекти

MKD-CIRT ќе ги доставува бараните информации на државни органи, јавни институции или на овластени трети страни секогаш кога постои законска обврска за тоа. Сепак, MKD-CIRT ќе го стори тоа само откако ќе се исполнат сите законски барања, на пр. достава на судски налог.

Секој случај на обработка или пренос на лични податоци според форма и содржина ќе биде во согласност со Законот за заштита на личните податоци, Законот за класифицирани информации Законот за електронските комуникации и другите важечки прописи во Република Македонија, при тоа имајќи ги предвид политиките и одлуките за класификација на информации на NATO и Европската унија.

4.3. Анонимизација

Осетливите информации најпрво ќе се анонимизираат пред истите да се споделат со трета страна. Нема да се разменуваат лични податоци (со кои може да се идентификува целта на компјутерскиот напад или било која индивидуа) или дополнителни податоци, без експлицитна писмена согласност на сопственикот на податоците или без претходна соодветна анонимизација на податоците. Овие информации може да се откријат на трета страна само доколку се неопходни за решавање на инцидент.

Кога анонимизирањето на информацијата не е практично или контра продуктивно во врска со справување со инцидентот, MKD-CIRT го задржува правото да сподели одредени не анонимизирани информации со групи или трети лица со кои има изградено доверба.

Овие размени на информации се извршуваат во согласност со важечките закони во Република Македонија и со експлицитно писмено одобрување од страна на сопственикот на информацијата што се разменува (Образец – Овластување за откривање на информација – Authorization to Disclose Information)

4.4. Користење на TLP за споделување на информации

4.4.1. Општи принципи

Со цел да ги заштити информациите, MKD-CIRT ќе ја применува својата внатрешна Политика за класификација на информации на MKD-CIRT. Тимот на MKD-CIRT при размена на информации ќе применува одредени правила кои се засновани на користење на општо прифатен и користен протокол TLP – Traffic Light Protocol.

MKD-CIRT ќе ги означува информациите што се разменуваат со соодветна ознака во согласност со TLP само при размена на информацијата со страна која го прифатила користењето на овој протокол. Доколку овој протокол не е поддржан од страната со која се размена информацијата, MKD-CIRT ќе примени проверка и усогласување на нивоата за класификација применети од двете страни, пред информацијата да биде споделена.

Правилата за класификација на информациите во согласност со TLP протоколот се дадени во Прилог – Користење на TLP (Traffic Light Protocol) за споделување на информации.

Секоја комуникација и размена на информација на ниво повисоко од ниво GREEN, особено пораките по електронска пошта, ќе бидат означени со ознака „[TLP Боја]“, каде Боја може да има вредност RED или AMBER.
Слична ознака или печат треба да е јасно видлива на корицата или заглавието од документите што ги испраќа или објавува MKD-CIRT. Доколку комуникацијата се врши преку телефонски разговор или видео конференциска врска, соодветното ниво за класификација на информацијата во согласност со TLP треба да се наведе на почетокот од разговорот, пред испорака на информацијата.

4.4.2. Стандардно TLP ниво на класификација

Како стандардно ниво за TLP класификација за откривање на информација ќе се користи [TLP AMBER] нивото за откривање на информација

Прилог – Користење на TLP (Traffic Light Protocol) за споделување на информации

Секоја информација при размената ќе биде задолжително означена со ознака во согласност со следната табела. Доколку информацијата што се разменува не е означена, MKD-CIRT ќе ја означи со ознака TLP AMBER :

Ознака	Објаснување за користење
TLP RED	Информација што не се открива и е ограничена само на претставници на учесниците во размената на информацијата. Претставниците не смеат да ја споделуваат информацијата надвор од учесниците на размената на оваа информација. За информација означена со ниво TLP RED може да се дискутира само за време на размената на оваа информација, кога сите учесници на размената на информацијата се согласни за тоа. Лица или страни кои не се учесници во размената на TLP RED информација НЕ СМЕАТ да присуствуваат на размената или дискусијата по информацијата.
TLP AMBER	Информацијата има ограничено откривање и е наменета само за членовите на информацискатa размена: членови на организации или конституенти (директно вработени лица, консултанти, или други ангажирани работници) кои го исполнуваат условот „ПОТРЕБНО Е ДА ЗНАЕ“ со цел да можат да постапат по информацијата.
TLP GREEN	Информацијата може да се споделува со други организации, при информациска размена со индивидуи и експерти во областа на информацискатa безбедност, но не смее да се објавува јавно и поставува на јавна веб-страница.
TLP WHITE	Јавна информација, нема ограничување во нејзината дисеминација, објава, поставување на јавни веб-страници или емитување. Секој член на Информацискатa размена може да ја објави информацијата со почитување на правата за заштита на интелектуална сопственост.