Национална таксономија за сајбер инциденти

(работна верзија, октомври 2019 година)

Вовед

Националната таксономија за сајбер-инциденти е активност предвидена со Акциски от план за имплементација на Стратегија за сајбер безбедност 2018 – 2022 година[1]. Во насока за реализација на Цел 1: Сајбер отпорност, дел за Унапредување на капацитетите и способностите на MKD-CIRT и развој на останатите CSIRT/CERT/CIRT тимови, дефинирана е задача 1.1.3 Развој на национална таксономија за сајбер инциденти.

Националниот центар за одговор на компјутерски инциденти MKD-CIRT како дел од Годишен извештај за работа за 2016 година, до Владата на Република Македонија достави таксономија за сајбер инциденти во склоп на документ Упатство за пријава на инциденти од конституенти, и истата е усвоена беше усвоена.

Задачата за Развој на Национална таксономија за сајбер инциденти е во насока на ревизија на постојната таксономија и вклучување на мислења од сите засегнати и заинтересирани страни, преку објава на предлог за Национална таксономија за сајбер инциденти. Со оваа таксономија ќе се овозможи сите чинители во областа на информациска и сајбер-безбедност да имаат изедначени критериуми при класификација на настаните во своите информациски системи и компјутерски мрежи и ќе овозможи успешно креирање и размена на информации за овие настани преку користење на заеднички јазик – „таксономија“.

По прифаќањето и усвојувањето на Национална таксономија за сајбер инциденти, ќе се исполнат предуслови сите организации од владиниот, јавниот и приватниот сектор, како и операторите на критична информациска инфраструктура во државата, кои разменуваат информации за настани поврзани со компјутерска безбедност, да имаат еднакво разбирање за случувањата и контекстот на настанот за кој се разменуваат информации.

По усвојување на таксономијата, MKD-CIRT ќе ги направи потребните ревизии во упатствата и процедурите за анонимна пријава на инциденти и упатството за пријава на инцидент од конституенти, како и во системите за пријава на инциденти и постапување по пријава на инцидент, како и во системите за размена на информации за инциденти и координација на одговор по сајбер-инцидент.

[1] Министерство за информатичко општество и администрација, http://www.mioa.gov.mk/?q=mk/node/1813

Таксономии за сајбер инциденти и сајбер напади

Во сајбер-просторот има повеќе чинители кои на различен начин ги обработуваат информациите поврзани со инциденти по компјутерска безбедност, т.е. сајбер-инциденти. Од овие причини, успешната класификација на сајбер-инцидентите е сложен процес. На пример, иако CIRT (анг. Computer Incident Response Team) и LEA (анг. Law Enforcement Agency, агенции за спроведување на закони) имаат иста заедничка цел – справување со сајбер-напади и инциденти, тие на различен начин доприносуваат во решавањето и истрагата по инцидентот. LEA собира информации кои може да се користат во тек на истрагата со цел да се утврдат доказите за извршување на кривично дело или за идентификација на напаѓачот, додека CIRT тимовите првенствено се насочени кон собирање на информации за моменталните закани и вектори на напад со цел нивно отстранување и понатамошно јакнење на отпорноста и превенцијата во сајбер-просторот.

Денес постојат повеќе таксономии што се користат како de-facto стандарди за таксономија и опис на сајбер-инцидентите. Една од најчесто користените таксономии која ENISA ја предлага како појдовна точка е таксономијата изработена од страна на eCSIRT.net во својата ревизија eCSIRT.net mkVI. Според ENISA, таксономијата треба да содржи:

- Класификациска шема – можност поврзани настани да се групираат
- Речник – опис на знаење и ентитети. Ова е од особено значење за нашата држава бидејќи во ИКТ речникот има многу странски поими што не можат прецизно да се преведат.
- Мапа на знаење – можност корисниците за кратко време да ја разберат целосната структура на сјабер-инцидент преку таксономијата

Во изработката на национална таксономија треба да се запазат горе наведените три карактеристики со цел истата да може да се користи од широк круг на идни корисници во Република Северна Македонија.

Национална таксономија за сајбер инциденти

Националната таксономија за сајбер инциденти се базира на референтната таксономија предложена од страна на ENISA[2], која е всушност таксономијата предложена од страна на eCSIRT.net[3]. Таксономијата овозможува категоризација на сајбер инцидентите според атрибутот „Оперативен ефект на напад“ како еден од петте атрибути кои ги пропишува т.н. AVOIDIT таксономија за сајбер-напади (анг. „AVOIDIT: A Cyber Attack Taxonomy“), развиена на Одделот за компјутерски науки при Универзитетот во Мемфис, САД (University of Memphis, Department of Computer Science). AVOIDIT методологијата овозможува прецизно идентификување на сајбер-нападите преку користење на пет атрибути:

- Вектор за напад
- Оперативен ефект на нападот
- Ефект на нападот врз информацијата
- Објект на напад, и
- Постигната фаза на нападот

[2] ENISA Reference Incident Classification Taxonomy, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

[3] http://www.ecsirt.net/

Прво (основно) ниво за категоризација на сајбер-инциденти

Следува поделба на сајбер-инцидентите според атрибутот „Оперативен ефект на нападот“ што ќе се користи како основа за националната таксономија на сајбер-инцидентите во прво ниво на поделба.

Националната таксономија за сајбер инциденти се состои од главни категории:

Класификација на инцидент	Пример за инцидент од наведената категорија	Опис
Навредлива содржина	Спам	Или „Несакана масовна е-пошта“, тоа значи дека примачот не дал потврда за дозвола за испраќање на пораката и дека пораката е испратена како дел од поголема колекција на пораки, сите имаат функционално споредлива содржина.
	Штетен говор	Дискредитација или дискриминација на лица, расизам или закани против едно или повеќе лица.
	Деца / Насилство	Детска порнографија, славење на насилство и сл.
Штетен код	Инфициран систем	Систем заразен со малвер, на пр. компјутер, паметен телефон или сервер заразен со rootkit.
	C&C сервер	Сервер за команда и контрола контактиран од малициозен софтвер на заразени системи.
	Дистрибуција на малвер	URI што се користи за дистрибуција на малициозен софтвер, на пр. URL-то за преземање вклучено во спам порака за лажни фактури.
	Конфигурација на малициозен софтвер	URI каде е поставена датотека за конфигурација на малициозен софтвер, на пр. за банкарски тројанец.
Прибирање на информации	Скенирање	Напади кои испраќаат барања до систем за да откријат слабости. Ова исто така вклучува процеси на тестирање за да се соберат информации за уредите, услугите и сметките. Примери: пребарување на DNS, ICMP, SMTP (EXPN, RCPT, ...), скенирање на порта.
	Снифинг (Sniffing)	Набудување и евидентирање на мрежниот сообраќај (прислушување).
	Социјален инженеринг	Собирање информации од лица на не технички начин (на пр. лаги, трикови, мито или закани).
Обиди за упад	Искористување на познати ранливости	Обид за компромитација на систем или за прекин на услуга преку искористување на ранливости со стандардизирани идентификатори како

		CVE - Common Vulnerabilities and Exposures
	Обиди за најава	Повеќе последователни обиди за најава (логирање) (Погодување или пробивање на лозинки, т.н. „brute force“ напади
	Нов потпис за напад (signature)	Обид
Упади	Компромитација на привилегирана сметка	Компромитација на механизми за автентикација и авторизација за пристап до услуги и информации заштитени со механизми за автентикација и авторизација на пристап и акции
	Компромитација на не привилегирана сметка	Неовластен пристап до услуги и информации кои не се заштитени со механизми за автентикација и авторизација на пристап и акции
	Компромитација на апликација	Неовластен пристап до апликативно ниво
	Бот	Компромитиран уред под контрола на криминалци поврзан на Интернет што може да се користи за штетни активности
Достапност	Denial of Service / Одбивање на услуга	
	Distributed Denial of Service / Дистрибуирано одбивање на услуга	
	Саботажа	
	Исклучување (без лоша намера)	
	Неавторизиран пристап до информација	
	Неавторизирана промена на информација	
	Неавторизирано користење на ресурси	
	Авторско право	
	Маскирање	
	Phishing / Фишинг	
Ранливост	Достапно за злоупотреба	
Друго		Сите инциденти кои не се дел од горе наведените категории треба да се стават во оваа категорија

Дополнителни нивоа на категоризација на инцидентите за подетален опис на инцидентот

Освен категоризација на инцидентите на прво ниво кое кореспондира на референтната таксономија за сајбер-инциденти на ENISA, националната таксономија може да се дополни со:

- Додавање на под класификации за атрибутот Оперативен ефект на напад, и/или
- Дополнување на категоризацијата со останатите 4 атрибути од AVOIDIT таксономијата

Сметајќи дека останатите 4 атрибути се зависни од времето на пријавување на инцидентот и/или се често променливи, националната таксономија предвидува додавање на вредностите за останатите 4 атрибути да се врши во облик на придружни информации и мета-податоци кон пријавата на инцидентот, кои во одредено време ќе се менуваат и/или дополнуваат.

Под ниво за класификација на инцидент според атрибутот „Оперативен ефект“

Основната категоризација на инцидентите според Оперативниот ефект може дополнително да се подели на следно под ниво, со предлог распределба даден во табелата во продолжение.

Основна категорија	Под категорија	Опис
Навредлива содржина	Спам	Несакана порака испратена по е-пошта која често содржи рекламен материјал
	Измама (анг. Hoax)	Порака испратена по е-пошта со лажна содржина, испратена со цел дезинформација или заплашување на примачот
	Деца	Детска порнографија
	Насилство	Величење на насилство
Штетен код	Малвер URL	Врска до поставен штетен програмски код на компромитирана веб-локација
	Фишинг URL	Врска до лажна интернет страница на компромитирана веб-локација чија цел е кражба на лични или осетливи податоци
	Спам URL	Врска до компромитирана веб-локација на веб-сервер со неовластено поставена рекламна содржина
	Веб-обезличување (web defacement)	Подразбира компромитирана веб-локација со променет изглед и содржина на веб-страница
	Систем заразен со штетен код	Подразбира компјутер (ПЦ, лаптоп, смартфон, таблет, IoT и др.) заразен со штетен код
	C&C	„Command and Control“ означува централна точка (сервер) за надзор и управување со уреди кои се дел од ботнет (анг. botnet). Истата може да се користит и за прибирање на украдени податоци од уредите – ботови.
	Корисничка сметка	Компромитација на корисничка сметка што се користи за пристап до веб-ресурси, услуги или уред.
Прибирање на информации	Скенирање	Напади кои испраќаат барања до систем за да откријат слабости. Ова исто така вклучува процеси на тестирање за да се соберат информации за уредите, услугите и сметките. Примери: пребарување на DNS, ICMP, SMTP (EXPN, RCPT, ...), скенирање на порта.

	Снифинг (Sniffing)	Набудување и евидентирање на мрежниот сообраќај (прислушување).
	Социјален инженеринг	Собирање информации од лица на не технички начин (на пр. лаги, трикови, мито или закани).
Обиди за упад	Искористување на познати ранливости	Обид за компромитација на систем или за прекин на услуга преку искористување на ранливости со стандардизирани идентификатори како CVE - Common Vulnerabilities and Exposures
	Обиди за најава	Повеќе последователни обиди за најава (логирање) (Погодување или пробивање на лозинки, т.н. „brute force“ напади
	Нов потпис за напад (signature)	Обид
Упади	Компромитација на привилегирана сметка	
	Компромитација на не привилегирана сметка	
	Компромитација на апликација	
	Бот	
Достапност	Denial of Service / Одбивање на услуга	
	Distributed Denial of Service / Дистрибуирано одбивање на услуга	
	Саботажа	
	Исклучување (без лоша намера)	
	Неавторизиран пристап до информација	
	Неавторизирана промена на информација	
	Неавторизирано користење на ресурси	
	Авторско право	
	Маскирање	
	Phishing / Фишинг	
Ранливост	Достапно за злоупотреба	
Друго		Сите инциденти кои не се дел од горе наведените категории треба да се стават во оваа категорија

Корелација на предложената таксономија со тековната таксономија користена во MKD-CIRT

На следната слика е дадена корелација на класификацијата што тековно се користи во MKD-CIRT и предложената таксономија усогласена со референтната таксономија на ENISA.

Национална таксономија за сајбер-инциденти

Основна категорија	Под категорија
Навредлива содржина	Спам
	Измама (анг. Hoax)
	Деца
	Насилство
Штетен код	Малвер URL
	Фишинг URL
	Спам URL
	Веб-обезличување (web defacement)
	Систем заразен со штетен код
	C&C
	Корисничка сметка
Прибирање на информации	Скенирање
	Снифинг (Sniffing)
	Социјален инженеринг
Обиди за упад	Искористување на познати ранливости
	Обиди за најава
	Нов потпис за напад (signature)
Упади	Компромитација на привилегирана сметка
	Компромитација на не привилегирана сметка
	Компромитација на апликација
	Бот
Достапност	Denial of Service / Одбивање на услуга
	Distributed Denial of Service / Дистрибуирано одбивање на услуга
	Саботажа
	Исклучување (без лоша намера)
	Неавторизиран пристап до информација
	Неавторизирана промена на информација
	Неавторизирано користење на ресурси
	Авторско право
	Маскирање
	Phishing / Фишинг
Ранливост	Достапно за злоупотреба
Друго	
Тест	Наменето за тестирање

Тековна таксономија што се користи во MKD-CIRT

Назив	Опис
Компромитирана информација	Успешно уништување, расипување, или откривање на чувствителни информации или интелектуална сопственост.
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.
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.
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 који успешно го ставил во карантин штетниот софтвер.
(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.
Кражба или загуба	Кражба или загуба на чувствителната опрема (лаптоп, хард диск, медиуми и др. опрема) на организацијата.
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
Незаконски активности	Измама /Човечка безбедност/ Детска порнографија. Компјутерски инциденти од криминална природа, најчесто со вклучена извршна власт, меѓународни истраги или превенција на губиток.
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 компромитација или одбивањето на услуга. (Denial of service).
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.