Nacionalna taksonomija računalno-sigurnosnih incidenata

Verzija 2

Ožujak 2019.

Sufinancira Europska unija
Instrument za povezivanje Europe

Projekt je sufinanciran sredstvima CEF - Connecting Europe Facility programa Europske komisije, broj ugovora: INEA/CEF/ICT/A2016/1334308 (Action No: 2016-HR-IA-0085)

Izjava o odricanju odgovornosti

Verzijom 2 izrađena je dopuna dokumenta Nacionalna taksonomija računalno-sigurnosnih incidenata objavljena 15. lipnja 2018. godine. Izmjene se odnose na dopune dijela Operativni učinak napada (O) koji se nalazi u tablici na stranici 8 ovog dokumenta. U izmjenama su sudjelovala tijela koja su nositelji Mjere G.1.1 Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti (Nacionalni CERT, ZSIS, HAKOM, HNB) te MUP RH kao tijelo koje koristi dio Nacionalne taksonomije u operativnom rješavanju incidenata.

Sadržaj

Pojmovi

U svrhu boljeg razumijevanja problematike iz domene kibernetičke sigurnosti odnosno računalnih ugroza informacijskih sustava koje dolaze iz kibernetičkog prostora (*eng. cyber space*) u ovom će se dokumentu definirati i pojasniti ključni pojmovi.

Kibernetički prostor (*eng. cyber space*) – prostor unutar kojeg se odvija komunikacija između informacijskih sustava. U kontekstu Nacionalne strategije kibernetičke sigurnosti RH obuhvaća internet i sve s njim povezane sustave.

Kibernetička sigurnost – obuhvaća aktivnosti i mjere kojima se postiže povjerljivost, cjelovitost i dostupnost podataka i sustava u kibernetičkom prostoru.

Kibernetički napad – zlonamjeran utjecaj na informacijske sustave, računalne mreže i ostale elektroničke resurse, koji se odvija u kibernetičkom prostoru s ciljem ugrožavanja povjerljivosti, cjelovitosti i dostupnosti podataka koji se na tim sustavima, mrežama i resursima stvaraju, obrađuju, pohranjuju i koji se putem njih prenose.

Kibernetički događaj – svaka pojava u računalnoj mreži ili informacijskom sustavu koju je moguće uočiti.

Prijetnja – potencijalni izvor neželjenog događaja.

Računalno-sigurnosni incident – jedan ili više računalno-sigurnosnih događaja koji su narušili odnosno narušavaju sigurnost informacijskog sustava ili računalne mreže, te ugrožavaju povjerljivost, cjelovitost i dostupnost informacija koje se korištenjem informacijskog sustava ili računalne mreže kreiraju, obrađuju, pohranjuju ili prenose.

Kibernetička kriza – događaj ili niz događaja u kibernetičkom prostoru, koji bi mogli uzrokovati ili su već prouzročili veći poremećaj u društvenom, političkom i ekonomskom životu RH. Takvo stanje u konačnici može utjecati na sigurnost ljudi, demokratski sustav, političku stabilnost, gospodarstvo, okoliš i druge nacionalne vrijednosti odnosno na nacionalnu sigurnost i obranu države općenito.

Taksonomija – znanost, tehnika ili metoda klasificiranja.

Vektor napada – opisuje način (put) na koji napadač ostvaruje inicijalni pristup sustavu.

Značajan incident – računalno-sigurnosni incident koji utječe na kritične podatke (neklasificirane i klasificirane) i/ili informacijske sustave i računalne mreže u javnom i privatnom sektoru, posebice na sustave koji su dio nacionalne kritične infrastrukture, na kojima se ti podaci obrađuju i kojima se prenose te koji može ostvariti i/ili ostvaruje negativan utjecaj na svakodnevni život velikog broja građana, nacionalnu ekonomiju i nacionalnu sigurnost u cjelini.

Uvod

Nacionalna taksonomija računalno-sigurnosnih incidenata nastala je temeljem Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti[1] (dalje u tekstu Akcijski plan). Poglavlje G navedenog Akcijskog plana odnosi se na tehničku koordinaciju u obradi računalno-sigurnosnog incidenta, a cilj G1 glasi: *„Kontinuirano unaprjeđivati postojeće sustave za prikupljanje, analizu i pohranu podataka o računalnim sigurnosnim incidentima te voditi brigu o ažurnosti drugih podataka bitnih za brzu i efikasnu obradu takvih incidenata".*

Prvi korak u provođenju ovog cilja definiranje je samog pojma računalno-sigurnosnog incidenta i njegove klasifikacije na nacionalnoj razini.

Kako bi svi dionici na području informacijske i kibernetičke sigurnosti (*eng. cyber security*) na nacionalnoj razini imali ujednačene kriterije pri klasifikaciji događaja u svojim informacijskim sustavima i računalnim mrežama te kako bi uspješno generirali i razmjenjivali informacije o tim događajima potrebno je utvrditi „zajednički jezik" – taksonomiju.

Stoga je prva mjera cilja G1 Akcijskog plana, mjera G.1.1, posvećena upravo tom zadatku, *„definiranju taksonomije, uključujući pojam značajnog incidenta".*

Nakon prihvaćanja i usvajanja Nacionalne taksonomije računalno-sigurnosnih incidenata (kasnije u tekstu Taksonomija) stvorit će se preduvjeti da sva tijela i institucije koje će razmjenjivati informacije o računalno-sigurnosnim događajima to čine tako da su svim sudionicima u toj razmjeni u potpunosti jasni i kontekst i detalji o pojedinom događaju ili incidentu.

Nadalje, prihvaćanjem ove Taksonomije bit će moguće započeti rad na ostalim dijelovima mjere G.1.1 koji uključuju *„definiranje protokola za razmjenu anonimiziranih podataka o značajnim sigurnosnim incidentima, te uspostaviti platformu ili tehnologiju za razmjenu podataka".* Bez prihvaćenog nacionalnog sustava klasifikacije, izgradnja platforme ili tehnologije za razmjenu podataka nije moguća.

[1] Nacionalna strategija kibernetičke sigurnosti i Akcijski plan za provedbu Nacionalne strategije kibernetičke sigurnosti http://narodne-novine.nn.hr/clanci/sluzbeni/2015_10_108_2106.html

Taksonomija računalno-sigurnosnih incidenata

Uspješna klasifikacija računalno-sigurnosnih incidenata složen je postupak budući da u kibernetičkom prostoru postoji više dionika koji kibernetičke događaje i računalno-sigurnosne incidente promatraju na različite načine. Na primjer, iako CERT-ovi (*eng. Computer Emergency Response Team*) i LEA (*eng. Law enforcement agency)* imaju isti zajednički cilj, oni na različiti način doprinose rješavanju i istrazi incidenata. LEA prikupljaju informacije koje se mogu koristiti tijekom istrage kako bi se utvrdili dokazi počinjenja kaznenog djela ili identificirao napadač, dok su CERT-ovi prvenstveno usmjereni na prikupljanje informacija o trenutačnim prijetnjama i vektorima napada s ciljem njihova otklanjanja te daljnjeg jačanja prevencije unutar kibernetičkog prostora.

Upravo iz tog razloga u ovom trenutku ne postoji standardizirana, međunarodno priznata taksonomija kibernetičkih događaja koja bi omogućila uspješnu i standardiziranu razmjenu informacija. Brojni znanstveni radovi posvećeni su ovoj problematici pa tako danas postoji više predloženih taksonomija koje se koriste isključivo u pojedinim organizacijama ili državama ili su usmjerene na određenu vrstu prijetnji (npr. taksonomija *DoS* napada).

Postoje tri bitna obilježja taksonomije prema ENISA-i[2]:

- Klasifikacijska shema – mogućnost da se povezani događaji svrstavaju u grupe.
- Rječnik – važan za opis znanja i entiteta. Ovo je obilježje osobito bitno u hrvatskom jeziku, budući da velik dio pojmova iz domene kibernetičke sigurnosti nije moguće precizno označiti.
- Mapa znanja – mogućnost da korisnici u kratkom roku mogu razumjeti cjelokupnu strukturu računalno-sigurnosnog incidenta obrađenog taksonomijom.

Izrada nacionalne taksonomije vođena je tako da zadovolji sva tri prethodno navedena obilježja te da bude prilagođena za korištenje što širem krugu budućih korisnika u Republici Hrvatskoj.

[2] https://www.enisa.europa.eu/

Razmjena informacija

Razmjena informacija predstavlja jedan od ključnih mehanizama uspješne obrane od kibernetičkih napada. Kibernetički prostor nije omeđen fizičkim barijerama te omogućava napadačima provođenje napada bez obzira na geografsku udaljenost čime je ujedno omogućeno i simultano provođenje napada na veći broj meta. Velik broj kibernetičkih napada, nakon što se pokažu uspješnim, koristi se dugi niz godina i s vremenom postaju sve sofisticiraniji. Iz svega navedenoga jasno je da razmjena informacija o kibernetičkim napadima i metodama obrane predstavlja važan dio mehanizma obrane od kibernetičkih prijetnji.

Osnovne karakteristike uspješne razmjene informacija su:

- Pravovremenost – informacija je vremenski korisna (stiže u pravo vrijeme)
- Točnost – informacija sadrži točne podatke
- Autentičnost – vjerodostojnost informacije nije upitna (izvor informacije je pouzdan).

Razmjena informacija postaje složena u situaciji kad informacije nisu prezentirane u standardiziranom obliku, a zahtijeva se brza razmjena i promptno djelovanje po primitku informacije. Upravo su brzina razmjene i promptno djelovanje osnovne značajke svakog sustava za razmjenu informacija. Potreba za standardiziranim oblikom prikaza i razmjene informacija nameće se kao prvi korak u izgradnji sustava za razmjenu informacija.

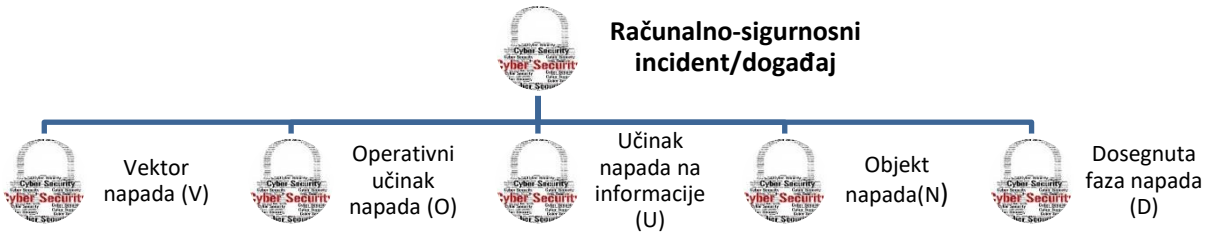
Nacionalna taksonomija RH (VOUND)

Nacionalna taksonomija RH izrađena je korištenjem modela javno objavljene AVOIDIT taksonomije (*eng. Attack Vector, Operational Impact, Defense, Information Impact, and Target*) razvijene na Odjelu za računalne znanosti Sveučilišta u Memphisu, SAD (*University of Memphis, Department of Computer Science*) uz uvažavanje iskustva i specifičnosti u obradi računalno-sigurnosnih incidenata u RH. Osnovna značajka AVOIDIT taksonomije jest u tome da se računalni događaj i/ili incident klasificira korištenjem više atributa. Korištenjem te metode omogućava se jako precizno definiranje i međusobno razlikovanje pojedinih događaja i incidenata.

Nacionalna taksonomija također se zasniva na korištenju atributa koji bi na nacionalnoj razini trebali omogućiti sveobuhvatni opis svih računalno-sigurnosnih incidenata i događaja čije uklanjanje zahtijeva razmjenu informacija i pravovremene odgovore nadležnih CERT timova.

Po uzoru na navedenu AVOIDIT taksonomiju, Nacionalna taksonomija računalno-sigurnosnih incidenta koristit će akronim **VOUND** dobiven korištenjem početnih slova ključnih riječi pet atributa predloženih za opis računalno-sigurnosnih incidenta u RH (Slika 1.):

- ***V**ektor napada*
- ***O**perativni učinak napada*
- ***U**činak napada na informacije*
- *Objekt **N**apada i*
- ***D**osegnuta faza napada.*



Slika 1. Atributi za opisivanje računalno-sigurnosnih incidenata

Taksonomija koja koristi gore navedene atribute ne podrazumijeva da je u svim slučajevima moguće pojedini događaj ili incident opisati jedinstvenom vrijednošću za svaki pojedini atribut. Kibernetički napad primjerice može koristiti više vektora napada u isto vrijeme te je korištenjem predložene metodologije moguće odabrati više vrijednosti pojedinog atributa za određeni događaj.

Korištenje Nacionalne taksonomije

Prihvaćena Taksonomija koristit će se na nacionalnoj razini od strane tvrtki iz različitih sektora, tijela državne uprave te ostalih pravnih i fizičkih osoba. Kako bi se omogućilo prikupljanje i razmjena informacija među svim dionicima koji će koristiti predloženu Taksonomiju, neovisno o razini znanja o računalno-sigurnosnim incidentima, te kako bi se omogućila adekvatna klasifikacija događaja/incidenata, na temelju eCSIRT.net[3] klasifikacije incidenta, definiran je minimalni set informacija (atribut Operativni učinak napada kojim se opisuje direktan utjecaj napada na informacijski sustav ili njegove dijelove) koje je potrebno prikupiti za svaki pojedini događaj/incident. Pri tome su u obzir uzeti sljedeći kriteriji:

1. jednostavno korištenje u svakodnevnom radu
2. jednoznačna klasifikacija računalno-sigurnosnog incidenta
3. jasna interpretacija klasificiranih računalno-sigurnosnih incidenta

Uz minimalni set informacija, koji je nužan za osnovnu klasifikaciju događaja/incidenata, taksonomija VOUND, omogućava korisnicima preciznije definiranje i međusobno razlikovanje pojedinih događaja i incidenata, a u ovisnosti o njihovoj razini znanja te dostupnim informacijama o računalno sigurnosnom događaju/incidentu. Opis događaja/incidenta upotrebom svih pet atributa iz Taksonomije, omogućava izradu preciznijih statističkih modela te potencijalno razvoj modela za rano uočavanje i sprječavanje zlonamjernih kampanja, kako je i opisano u poglavlju Mogućnosti daljnje razrade i primjene u budućnosti.

Vektor napada (V)

Vektor napada koristi se kao atribut opisa računalno-sigurnosnog incidenta kako bi se shvatio i opisao način (put) na koji napadač ostvaruje inicijalni pristup sustavu. Identifikacija atributa Vektor napada može predstavljati izazov osobito kod napada visokog stupnja kompleksnosti gdje napadači posvećuju izuzetnu pažnju prikrivanju svakog koraka napada, pa se tako i Vektor napada u velikom postotku slučajeva čini kao legitiman ili uobičajen tijek događaja.

Tijekom napada nije neuobičajeno da napadači koriste više dostupnih vektora, ovisno o postojećim ranjivostima mete, pa ovaj atribut ne predstavlja „jedinstveni ključ" u identifikaciji napada. Identifikacija i razumijevanje atributa Vektor napada vrlo često može predstavljati jedan od ključnih koraka u atribuciji napada.

[3] https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf

Vrijednosti koje ovaj atribut može poprimiti su sljedeće.

Oznaka	Vrijednost	Opis
(V1)	Prijenosni mediji/uređaji	Napad je izveden korištenjem prijenosnog medija ili perifernog uređaja. Primjer: • Širenje zlonamjernog koda putem zaraženog USB-a ili CD/DVD-a.
(V2)	Napad na *web* tehnologije	Napad je izvršen korištenjem metoda povezanih s *web* tehnologijama i ranjivostima *web* aplikacija. Ovaj vektor napada između ostalog podrazumijeva: • *XSS* • *SQL Injection* • *DNS Hijacking* • *Brute force* napadi na autentifikacijske mehanizme *web* aplikacija, zaporke, *CAPTCHA* zaštitu ili digitalne potpise • Napad na internetske preglednike u korisničkom okruženju.
(V3)	Napad na dostupnu mrežnu i računalnu opremu	Napad koji iskorištava ranjivosti računalnih mreža, ranjivih mrežnih uređaja, javno dostupnih poslužitelja ili računala. Ovaj vektor napada podrazumijeva između ostalog: • *(D)DoS* • *Man-In-The-Middle* • Skeniranje javno dostupnih resursa • Lažne *wireless* pristupne točke • Utjecaj na otvorene portove javno izloženih poslužitelja.
(V4)	Fizički napad	Gubitak ili krađa opreme, računala ili medija za pohranu podataka. Namjerno ili nenamjerno fizičko djelovanje na opremu, računala ili medije. Ovaj vektor napada podrazumijeva između ostalog: • Otuđenje i instalaciju zlonamjernoga koda na prijenosna računala, mobilne uređaje i sl. • Instalaciju zlonamjernoga koda ili uređaja na fizički izložene uređaje kao što su bankomati, POS uređaji i sl. • Instalaciju zlonamjernoga koda ili zlonamjernih dijelova operativnog sustava prilikom proizvodnje ili isporuke računalne opreme.
(V5)	Socijalni inženjering	Vektor napada koji se oslanja na ljudsku interakciju i najčešće uključuje navođenje ljudi na kršenje uobičajenih sigurnosnih procedura. Ovaj vektor napada podrazumijeva između ostalog: • Pokušaj otkrivanja povjerljivih informacija lažnim predstavljanjem • *Phishing* – slanje e-mail ili SMS poruka s priloženim zlonamjernim dokumentima ili poveznicama na zlonamjerne *web* sadržaje • Navođenje na preuzimanje zlonamjernog sadržaja, zlonamjernih mobilnih aplikacija i sl.

(V6)	Napad iz unutrašnjeg okruženja	Napad koji uključuje korištenje informacija, pristupnih podataka i resursa dostupnih isključivo legitimnom korisniku koji te resurse koristi u zlonamjerne svrhe ili suprotno internim politikama i standardima.
(V7)	Nepoznato	Rana faza otkrivanja incidenta u kojem još nije poznat vektor napada.

Operativni učinak napada (O)

Klasifikacija napada prema operativnom učinku predstavlja atribut kojim se opisuje direktan utjecaj napada na informacijski sustav ili njegove dijelove.

Atribut Operativni učinak napada određen je kao osnovni set informacija koje je potrebno prikupiti jer daje odgovor na pitanje što se zapravo dogodilo s napadnutim informacijskim sustavom ili računalnom mrežom. Identifikacija atributa Operativnog učinka napada djelomično odgovara i na pitanje koja je motivacija i krajnji cilj napadača u provođenju napada.

U dolje priloženoj tablici navedene su vrijednosti koje ovaj atribut može poprimiti. Tijekom konkretnog napada atribut Operativnog učinka napada najčešće preuzima različite vrijednosti ovisno o fazi napada, pa tako najčešće „Prikupljanje informacija" u kasnijoj fazi napada prelazi u vrijednost „Kompromitacija" ili „Pokušaj neovlaštenog pristupa". Iz tog je razloga često nemoguće nedvosmisleno identificirati vrijednost ovog atributa.

Oznaka	Vrijednost	Oznaka	Potkategorije	Opis
(O1)	Uspješno ostvarena kompromitacija	(O11)	*Malware URL*	Poveznica do postavljenog zlonamjernog programskog koda na kompromitiranom web sjedištu.
		(O12)	*Phishing URL*	Poveznica do lažne Internet stranice na kompromitiranom web sjedištu čija je svrha krađa povjerljivih podataka.
		(O13)	*Spam URL*	Poveznica do kompromitiranog web sjedišta na web poslužitelju s neovlašteno postavljenim reklamnim sadržajem.
		(O14)	*Web Defacement*	*Web Defacement* podrazumijeva kompromitirano *web* sjedište s izmijenjenim izgledom i sadržajem *web* stranice.
		(O15)	Sustav zaražen zlonamjernim kodom	Podrazumijeva računalo (npr. PC, pametni telefon, IoT i sl.) zaraženo zlonamjernim kodom.
		(O16)	*C&C*	*C&C* podrazumijeva upravljački poslužitelj za nadzor i upravljanje računalima koja su dio botneta. Također može služiti kao točka

				prikupljanja ukradenih podataka s različitih botova.
		(017)	Korisnički račun	Korisnički račun podrazumijeva kompromitaciju korisničkog računa za pristup nekom web servisu ili računalnom sustavu.
(02)	Pokušaj neovlaštenog pristupa	(021)	Pogađanje zaporki	Pogađanje zaporki podrazumijeva neovlašten pokušaj pristupa računalnom sustavu višestrukim pogađanjem zaporke.
		(022)	Pokušaj iskorištavanja ranjivosti	Pokušaj iskorištavanja ranjivosti podrazumijeva pokušaj iskorištavanja ranjivosti na računalnom sustavu kako bi se ostvario neovlašten pristup ili utjecalo na tajnost ili cjelovitost podataka.
(03)	Prikupljanje informacija	(031)	Skeniranje	Skeniranje podrazumijeva neovlašteno automatizirano prikupljanje informacija o računalnim mrežama i sustavima.
		(032)	*Sniffing*	*Sniffing* podrazumijeva neovlašteno presretanje mrežnog prometa.
(04)	Dostupnost	(041)	DoS - Volumetrički napad	Volumetrički napad podrazumijeva napad slanjem velikog broja IP paketa s ciljem zagušenja mrežne propusnosti.
		(042)	DoS - Napad na aplikacijskom sloju	Napad na aplikacijskom sloju podrazumijeva slanje većeg broja zahtjeva prema računalnom sustavu s ciljem iskorištavanja resursa sustava ili iskorištavanje sigurnosnog propusta koje dovodi do prestanka rada aplikacije.
		(043)	Ispad usluge (eng. *Outage*)	Podrazumijeva neočekivani gubitak dostupnosti izazvan greškom u radu sustava, ljudskom greškom ili namjernim lokalnim sabotiranjem sustava. ***Ovaj tip incidenta odnosi se isključivo na tijela definirana Zakonom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018).***

(05)	Zlonamjerno rudarenje kriptovalute (eng. *Cryptojacking*)			Neovlašteno iskorištavanje CPU resursa korisničkog računala ili mobilnog uređaja za rudarenje kriptovalute. Najčešći oblici vektora *cryptojacking* napada dolaze putem *phishing* poruka (neopreznim pokretanjem poveznice ili privitka sa zlonamjernom *cryptomining* skriptom) ili prilikom posjete web sjedištu koje ima ugrađenu *cryptomining* skriptu (JavaScript).
(06)	Neželjene elektroničke poruke, uvredljiv sadržaj, uznemiravanje, dezinformiranje	(061)	*Spam*	*Spam* podrazumijeva neželjenu elektroničku poruku reklamnog sadržaja.
		(062)	*Hoax*	*Hoax* podrazumijeva poruku elektroničke pošte neistinitog sadržaja, poslana s ciljem zastrašivanja ili dezinformiranja primatelja.
(07)	Ciljani napad – *APT* (*eng. Advanced persistent threat*)			*APT* podrazumijeva ciljani napad na određenu žrtvu uz korištenje većeg broja naprednih tehnika i tehnologija.
(08)	Prijevare	(081)	*Phishing*	• Pokušaj navođenja korisnika na odavanje povjerljivih podataka putem raznih komunikacijskih kanala (najčešće elektroničke pošte). • Pokušaj navođenja korisnika na pokretanje zlonamjernog programa putem raznih komunikacijskih kanala (najčešće elektroničke pošte). • Napad u kojima napadač lažnim predstavljanjem pokušava steći financijsku korist od ciljane žrtve. Jedan on najčešćih oblika ovakvih napada su tzv. „CEO *fraud*“ ili „BEC“ (*Business Email Compromise*) elektroničke poruke.
		(082)	*Scam*	Pokušaji vještog navođenja potencijalne žrtve na djelovanje u korist prevaranta (najčešće putem elektroničke pošte). Najpoznatiji oblik je „*nigerian scam*“ ili „*419 fraud*“.

(09)	Ostalo			Podrazumijeva neželjene događaje koji ne mogu biti opisani ranije navedenim atributima, a koji bi se mogli okarakterizirati kao računalno-sigurnosni incident.

Učinak napada na informacije (U)

Krajnji cilj svakog kibernetičkog napada ostvarivanje je učinka na podatke/informacije u smislu narušavanja jednog od tri osnovna načela informacijske sigurnosti: povjerljivosti, cjelovitosti i dostupnosti podataka.

Kroz atribut Učinak napada na informacije klasificira se utjecaj napada na štićene informacije te pojašnjava kriterije za odabir pojedine vrijednosti atributa.

Oznaka	Vrijednost	Opis
(U1)	Izmjena/Iskrivljavanje	Narušavanje cjelovitosti informacije, uobičajeno tako da tijekom napada dođe do promjene ili "iskrivljavanja" podataka.
(U2)	Nedostupnost (Uskraćivanje pristupa ili sl.)	Uskraćivanje dostupnosti servisa koji omogućava pristup informaciji, uobičajeno uslijed *(D)DoS* napada.
(U3)	Uništenje	Do uništenja informacija uobičajeno dolazi kada napad za konačni cilj ima brisanje podataka ili uklanjanje pristupnih prava.
(U4)	Otkrivanje	Otkrivanje informacija podrazumijeva situaciju u kojoj napadač ostvari "uvid" u informacije kojima u normalnim okolnostima ne bi imao pravo pristupa.
(U5)	Nepoznato	Rana faza otkrivanja incidenta u kojoj još nije poznat učinak napada na informacije.

Objekt napada (N)

Kroz atribut Objekt napada klasificira se vrsta informacijske infrastrukture koja je meta kibernetičkog napada. Ispravnom klasifikacijom ovog atributa moguće je donijeti zaključke o motivima napadača te o budućem tijeku širenja incidenta.

Slično kao i kod atributa Operativni učinak napada i ovaj atribut najčešće mijenja vrijednost ovisno o fazi napada, a uslijed lateralnog „kretanja“ napadača nakon što uspješno ostvari neovlašten pristup prvotnom objektu napada. Iz tog je razloga često nemoguće nedvosmisleno identificirati vrijednost ovog atributa. Ovaj atribut može biti osobito dvosmislen kod *(D)DoS* napada kada najčešće nije u potpunosti jasno je li objekt napada računalna mreža ili aplikacijski sustav.

Oznaka	Vrijednost	Opis

(N1)	Upravljačka infrastruktura	Napad na kritične dijelove sustava koji koordiniraju aktivnosti i upravljaju resursima informacijskog sustava (npr. *Active Directory*).
(N2)	Računalna mreža	Napad na mrežnu infrastrukturu.
(N3)	Lokalno računalo	Napad kojem je krajnji cilj kompromitacija lokalnog računala (pojedinačnog korisnika).
(N4)	Korisnik	Napad na korisnika predstavlja napad koji za cilj ima prikupljanje korisnikovih osobnih informacija.
(N5)	Aplikacijski sustav	Napad na aplikacijski sustav predstavlja napad na specifičnu aplikaciju ili njen dio u svrhu uskraćivanja dostupnosti, kompromitacije podataka ili daljnjeg širenja opsega napada.
(N6)	Ostalo	Objekt napada koji nije opisan prethodno definiranim vrijednostima.

Dosegnuta faza napada (D)

Kroz atribut Dosegnuta faza napada identificira se trenutačni stadij kibernetičkog napada. Iako se u stvarnim situacijama faze kibernetičkog napada najčešće izmjenjuju u jako kratkim vremenskim intervalima, moguće je identificirati trenutačnu fazu u kojoj se zlonamjerni akteri i zlonamjerna kampanja nalaze. Ispravnom i pravovremenom klasifikacijom ovog atributa moguće je donijeti odluke o obrambenim strategijama koje mogu spriječiti napadača u prelasku u daljnje faze napada, nakon čega obrambeno djelovanje može imati bitno sužen skup mogućnosti.

Oznaka	**Vrijednost**	**Opis**
(D1)	Izviđanje	Faza napada u kojoj napadač prikuplja informacije o meti i priprema strategiju napada ovisno o otkrivenim ranjivostima. Ova faza najčešće uključuje skeniranje automatiziranim alatima, prikupljanje e-mail kontakata za potencijalnu upotrebu mehanizama socijalnog inženjeringa i sl.
(D2)	Isporuka	Faza napada u kojoj napadač aktivira mehanizme provođenja kibernetičkog napada. Ovu fazu uobičajeno obilježava slanje e-mail poruka sa zlonamjernim sadržajem ako se radi o kibernetičkom napadu koji koristi zlonamjeran kod ili pokretanje alata za generiranje zlonamjernih upita ako se radi o napadu uskraćivanja dostupnosti.
(D3)	Ostvarivanje pristupa	Faza napada u kojoj napadač iskorištava uočene ranjivosti sustava i ostvaruje pristup ciljanom sustavu. Uobičajeno, napadač u ovoj fazi instalira zlonamjeran kod, maksimalno eskalira privilegije, ovisno o cilju proširuje djelokrug napada širenjem na povezane sustave i računala i sl.
(D4)	Potpuna kompromitacija	Završna faza napada iz perspektive napadača u kojoj se ostvaruju ciljevi i motivacija za napad. Ova faza uobičajeno podrazumijeva eksfiltraciju, uništenje ili izmjenu podataka, uskraćivanje usluge i servisa,

		pokretanje novih napada korištenjem resursa kompromitiranog sustava i sl.
(D5)	Perzistencija	Faza napada u kojoj napadači ostvaruju trajnu prisutnost u kompromitiranom sustavu uz aktivirane sposobnosti sprječavanja detekcije.
(D6)	Nepoznato	Nije moguće odrediti fazu napada.

Mogućnosti daljnje razrade i primjene u budućnosti

Prihvaćenu Taksonomiju je potrebno koristiti kao alat koji će omogućiti efikasnu razmjenu informacija u svrhu bržeg uočavanja i sprječavanja računalno-sigurnosnih incidenta. Nacionalna taksonomija računalno-sigurnosnih incidenata:

1. Omogućava brzu identifikaciju i opis računalno-sigurnosnog incidenta i događaja kroz pet atributa karakterističnih za svaki kibernetički napad (primjeri u Prilogu 1).
2. Otvara prostor za dodatnu nadogradnju pojedinih atributa u slučajevima pojave novih vrsta prijetnji (npr. nova vrsta vektora napada).
3. Korištenjem opisanih pet atributa omogućava izradu detaljnih statističkih izvještaja unutar pojedine organizacije ili na nacionalnoj razini za potrebu praćenja trendova i uspješnosti korištenja obrambenih mehanizama.
4. Korištenjem atributa Objekt napada i Dosegnuta faza napada omogućava praćenje tijeka napada ili kampanje uz mogućnost brzog predviđanja sljedećeg koraka napadača (primjeri u Prilogu 2).

Postoje smjerovi koji primarno nisu u opsegu izvornog cilja uspostave sustava za razmjenu informacija i razvoja Nacionalne taksonomije računalno-sigurnosnih incidenata, ali se mogu razmatrati kao nadogradnja i budući smjerovi razvoja.

1. Planiranje sustava nacionalne procjene rizika kibernetičkih napada temeljem predložene taksonomije – ispravnom identifikacijom atributa taksonomije i korelacijom s „vrijednošću" i značajem konkretne mete moguće je procjenjivati rizik pojedinog računalno-sigurnosnog incidenta. Također, moguće je provesti i integraciju sa sustavom klasifikacije incidenata/događaja *Traffic Light Protocol* (*TLP*[4]). *TLP* pruža jednostavnu i intuitivnu klasifikacijsku shemu koja ukazuje na uvjete pod kojima se osjetljive informacije mogu dijeliti.
2. Automatizacija – potencijalnim automatiziranjem postupka prepoznavanja incidenta i klasificiranjem kroz predloženu taksonomiju moguće je izgraditi sustav predlaganja strategije i mehanizma obrane u ranoj fazi kibernetičkog napada. Nakon što sustav razmjene informacija, temeljen na predloženoj taksonomiji, postane opće prihvaćen i procesira veći broj događaja i incidenata bit će moguće iskoristiti

[4] *Traffic Light Protocol* (*TLP*) – predstavlja način na koji netko tko dijeli informacije obavještava primatelje o ograničenjima u daljnjem dijeljenju navedene informacije. Više o *TLP*-u na ovoj poveznici https://www.first.org/tlp/

prikupljeno znanje te odmah po prijavi događaja ili incidenta donositi određene zaključke o akterima, strategiji obrane i utjecaju na cjelokupnu razinu sigurnosti.

Prilog 1 – Identifikacija poznatih računalno-sigurnosnih incidenata primjenom atributa Operativni učinak

Tip ugroze	Vrijednost	Potkategorija
Ransomware – šifriranje podataka	Kompromitacija	Sustav zaražen zlonamjernim kodom
Web Defacement	Kompromitacija	*Web Defacement*
Skeniranje mreže nmap alatom	Prikupljanje informacija	Skeniranje
Phishing stranica	Kompromitacija	*Phsihing URL*
Zeus upravljački poslužitelj	Kompromitacija	*C&C*
Phishing kampanja	Prikupljanje informacija	*Phishing*
Spam kampanja	Neželjene elektroničke poruke, uvredljiv sadržaj, uznemiravanje, dezinformiranje	*Spam*
Kompromitiran Gmail račun	Kompromitacija	Korisnički račun
SYN flood	Uskraćivanje dostupnosti	Volumetrički napad
Brute force	Pokušaj neovlaštenog pristupa	Pogađanje zaporki
Mirai bot	Kompromitacija	Sustav zaražen zlonamjernim kodom

Prilog 2 – Identifikacija poznatih računalno-sigurnosnih incidenata primjenom pet atributa taksonomije VOUND

Zeus kampanja

Vektor napada (V)	Operativni učinak napada (O)	Učinak napada na informacije (U)	Objekt napada (N)	Dosegnuta faza napada (D)
Socijalni inženjering (5)	Kompromitacija/Sustav zaražen zlonamjernim kodom (1/5)	Otkrivanje (4)	Korisnik (4)	Kompromitacija (4)

V5_O15_U4_N4_D4

Ransomware – šifriranje podataka

Vektor napada (V)	Operativni učinak napada (O)	Učinak napada na informacije (U)	Objekt napada (N)	Dosegnuta faza napada (D)
Socijalni inženjering (5)	Kompromitacija/Sustav zaražen zlonamjernim kodom (1/5)	Uništenje (3)	Lokalno računalo (3)	Kompromitacija (4)

V5_O15_U3_N3_D4

Ransomware – šifriranje konfiguracijskih datoteka

Vektor napada (V)	Operativni učinak napada (O)	Učinak napada na informacije (U)	Objekt napada (N)	Dosegnuta faza napada (D)
Socijalni inženjering (5)	Kompromitacija/Sustav zaražen zlonamjernim kodom (1/5)	Prekid (2)	Upravljačka infrastruktura (1)	Kompromitacija (4)

V5_O15_U2_N1_D4

Web Defacement

Vektor napada (V)	Operativni učinak napada (O)	Učinak napada na informacije (U)	Objekt napada (N)	Dosegnuta faza napada (D)
Napad na *web* tehnologije(2)	Kompromitacija/ *Web Defacement* (1/4)	Iskrivljavanje (1)	Aplikacijski sustav (5)	Kompromitacija (4)

V2_O14_U1_N5_D4

Skeniranje

Vektor napada (V)	Operativni učinak napada (O)	Učinak napada na informacije (U)	Objekt napada (N)	Dosegnuta faza napada (D)
Napad na mrežnu opremu (3)	Prikupljanje informacija/Skeniranje (2/1)	Otkrivanje (4)	Računalna mreža (2)	Izviđanje (1)

V3_O21_U4_N2_D1

DDoS – SYN flood

Vektor napada (V)	Operativni učinak napada (O)	Učinak napada na informacije (U)	Objekt napada (N)	Dosegnuta faza napada (D)
Napad na mrežnu opremu (3)	Uskraćivanje dostupnosti/ Volumetrički napad (4/1)	Prekid (2)	Računalna mreža (2)	Kompromitacija (4)

V3_O41_U2_N2_D4

Prilog 3 – Praćenje tijeka napada i predviđanje sljedećih koraka napadača korištenjem pet atributa taksonomije VOUND

Primjer – Tijek *Spyware* kampanje

Početak napada obilježava kompromitacija korisničkog računala koje ne mora nužno biti krajnji cilj napada.

Vektor napada (V)	Operativni učinak napada (O)	Učinak napada na informacije (U)	Objekt napada (N)	Dosegnuta faza napada (D)
Socijalni inženjering (5)	Kompromitacija/Sustav zaražen zlonamjernim kodom (1/5)	Otkrivanje (4)	Korisničko računalo (3)	Kompromitacija (4)

V5_O15_U4_N3_D4

U sljedećoj fazi napada, napadači pokušavaju izvršiti daljnje širenje po mreži i kompromitaciju upravljačke infrastrukture pa se atribut Objekt napada mijenja u vrijednost „Upravljačka infrastruktura".

Vektor napada (V)	Operativni učinak napada (O)	Učinak napada na informacije (U)	Objekt napada (N)	Dosegnuta faza napada (D)
Socijalni inženjering (5)	Kompromitacija/Sustav zaražen zlonamjernim kodom (1/5)	Otkrivanje (4)	Upravljačka infrastruktura (1)	Kompromitacija (4)

V5_O15_U4_N1_D4

U slučaju uspješne identifikacije i klasifikacije napada, a uz sumirana znanja i iskustva o prethodnim napadima i kampanjama, moguće je prije prijelaza iz faze 1 u fazu 2 definirati i provesti strategiju obrane i/ili daljnjih aktivnosti.

Faza 1 V4_O1_U4_**N3**_D4

↓ Strategija obrane: Ukloniti kompromitirano računalo s mreže

Faza 2 V4_O1_U4_**N1**_D4

Korištenjem ovog principa moguće je prepoznavati i identificirati odnose (*eng. parent-child)* među događajima te tako bolje razumijevati dinamiku napada ili kampanje.