Nacionalna taksonomija kibernetičkih incidenata

Sadržaj

Pojmovi

U svrhu boljeg razumijevanja dokumenta navode se definicije i pojašnjenja ključnih pojmova.

Kibernetički prostor – 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 – je kibernetička sigurnost kako je definirana u članku 2. točki 1. Uredbe (EU) 2019/881.

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.

Kibernetička prijetnja – kibernetička prijetnja kako je definirana u članku 2. točki 8. Uredbe (EU) 2019/881.

Kibernetički incident – događaj koji ugrožava dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili usluga koje mrežni i informacijski sustavi nude ili kojima omogućuju pristup.

Kibernetička kriza – stanje koje može nastati u suvremenom društvu zbog visokog stupnja ovisnosti o mrežnim i informacijskim sustavima, a uslijed čega sve veći broj incidenata i napada može uzrokovati ozbiljne poremećaje u društvenom, političkom i ekonomskom smislu i time utjecati na sigurnost ljudi, demokratski sustav, političku stabilnost, gospodarstvo, okoliš i druge nacionalne vrijednosti, odnosno općenito na nacionalnu sigurnost RH.

Taksonomija – znanost, tehnika ili metoda klasificiranja.

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

Kibernetički sigurnosni incident velikih razmjera – incident na razini Europske unije koji uzrokuje poremećaje koji premašuju sposobnost jedne države članice za odgovor na incident ili koji ima znatan učinak na najmanje dvije države članice, kao i incident na nacionalnoj razini koji uzrokuje poremećaje koji premašuju sposobnost sektorskog CSIRT tijela za odgovor na incident ili koji ima znatan učinak na najmanje dva sektora te se u takvim slučajevima pokreću procedure upravljanja kibernetičkim krizama, usklađene s postojećim nacionalnim općim okvirom upravljanja krizama i okvirom za upravljanje kibernetičkim krizama Europske unije.

Uvod

Nacionalna taksonomija kibernetičkih incidenata (u daljnjem tekstu: Nacionalna taksonomija) predstavlja nacionalni sustav klasifikacije sigurnosnih incidenata.

Nacionalnu taksonomiju donosi središnje državno tijelo za kibernetičku sigurnost, na prijedlog nadležnih CSIRT-ova, a na temelju odredbe članka 78. Uredbe o kibernetičkoj sigurnosti („Narodne novine“, br. 135/24., u daljnjem tekstu: UKS).

Nacionalna taksonomija izrađena je dopunom Nacionalne taksonomije računalno-sigurnosnih incidenata izvorno objavljene 15. lipnja 2018. godine, izmijenjene u ožujku 2019. godine i prosincu 2021. godine.

Zakon o kibernetičkoj sigurnosti („Narodne novine“, br. 14/24., u daljnjem tekstu: ZKS) definira i uključuje različite dionike u sustav kibernetičke sigurnosti Republike Hrvatske (u daljnjem tekstu: RH). Nacionalna taksonomija omogućuje dosljedno evidentiranje, analizu i razmjenu informacija o incidentima između tih dionika, s ciljem unaprjeđenja kibernetičke sigurnosti i odgovora na prijetnje.

Ključni i važni subjekti kategorizirani ZKS-om, dužni su nadležni CSIRT (eng. *Computer Security Incident Response Team*), obavijestiti o svakom značajnom incidentu. Nadležni CSIRT po zaprimanju obavijesti o incidentu provodi analizu i klasifikaciju incidenta prema Nacionalnoj taksonomiji.

Taksonomija kibernetičkih incidenata

Uspješna klasifikacija kibernetičkih incidenata složen je postupak budući da u kibernetičkom prostoru postoji više dionika koji kibernetičke događaje i incidente promatraju na različite načine.

Na primjer, iako CSIRT-ovi i tijela kaznenog progona imaju isti zajednički cilj u pogledu kibernetičkih incidenata, oni na različiti način doprinose rješavanju i istrazi tih incidenata. Tijela kaznenog progona prikupljaju informacije koje se mogu koristiti tijekom istrage kako bi se utvrdili dokazi počinjenja kaznenog djela ili identificirao napadač, dok su CSIRT-ovi prvenstveno usmjereni na prikupljanje informacija o trenutačnim prijetnjama i vektorima napada s ciljem njihova otklanjanja te daljnjeg jačanja prevencije unutar kibernetičkog prostora.

Ne postoji standardizirana, međunarodno priznata taksonomija kibernetičkih događaja koja bi omogućila uspješnu i standardiziranu razmjenu informacija, ali postoje općenita, bitna obilježja koja svaka taksonomija kibernetičkih događaja mora sadržavati.

Prema ENISA-i[1] tri su bitna obilježja taksonomije:

- Klasifikacijska shema – mogućnost da se povezani događaji svrstavaju u grupe
- Rječnik – važan za opis znanja i entiteta
- Mapa znanja – mogućnost da korisnici u kratkom roku mogu razumjeti cjelokupnu strukturu kibernetičkog incidenta obrađenog taksonomijom.

Nacionalna taksonomija izrađena je tako da zadovoljava sva tri prethodno navedena obilježja i da bude prilagođena za korištenje što širem krugu budućih korisnika u RH.

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

Razmjena informacija

Razmjena informacija predstavlja jedan od ključnih mehanizama uspješne obrane od kibernetičkih napada.

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. Stoga se potreba za standardiziranim oblikom prikaza i razmjene informacija nameće kao prvi korak u izgradnji sustava za razmjenu informacija.

Atributi nacionalne taksonomije

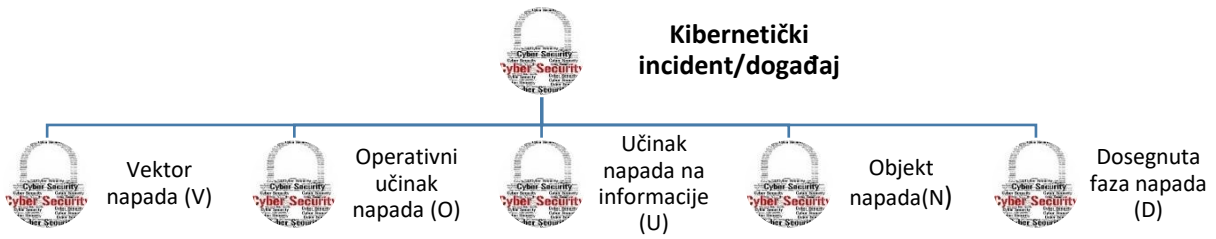
Nacionalna taksonomija je izrađena korištenjem modela javno objavljene AVOIDIT taksonomije (eng. *Attack Vector, Operational Impact, Defense, Information Impact, and Target*) razvijene na Odjelu za računalne znanosti Sveučilišta u Memphisu, SAD (*University of Memphis, Department of Computer Science*), uz uvažavanje iskustva i specifičnosti u obradi kibernetičkih incidenata u RH.

Osnovna značajka AVOIDIT taksonomije jest u tome da se računalni događaj i/ili incident klasificira korištenjem više atributa. Korištenjem te taksonomije omogućava se jako precizno definiranje i međusobno razlikovanje pojedinih događaja i incidenata.

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

Po uzoru na navedenu AVOIDIT taksonomiju, Nacionalna taksonomija će koristiti akronim **VOUND** dobiven korištenjem početnih slova ključnih riječi pet atributa predloženih za opis kibernetičkih 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 kibernetičkih 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 taksonomije moguće odabrati više vrijednosti pojedinog atributa za određeni događaj.

Korištenje Nacionalne taksonomije

Nacionalnu taksonomiju koristit će prvenstveno CSIRT-ovi, obveznici i nadležna tijela ZKS-a te ostale pravne i fizičke osobe u RH, kako bi se omogućilo prikupljanje i razmjena informacija neovisno o razini znanja o kibernetičkim incidentima te adekvatna klasifikacija događaja/incidenata.

Na temelju eCSIRT.net[2] klasifikacije incidenta definiran je minimalni set informacija (atribut Operativni učinak napada kojim se opisuje izravan 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 kibernetičkog incidenta
3. jasna interpretacija klasificiranih kibernetičkih 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 kibernetičkom događaju/incidentu. Opis događaja/incidenta upotrebom svih pet atributa iz Nacionalne 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 kibernetičkog 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.

Vrijednosti koje ovaj atribut može poprimiti su sljedeće:

Oznaka	Vrijednost	Opis
(V1)	Prijenosni mediji/uređaji	Napad je izveden korištenjem prijenosnog medija ili perifernog uređaja. Ovaj vektor napada primjerice podrazumijeva: • 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*

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

		• *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 minimalni 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 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	Potkategorije		Opis
(O1)	Napadačka infrastruktura			Obuhvaća prijave u kojima nije nužno detektiran napad, već je otkrivena infrastruktura koja se koristi za kibernetičke napade, poput C2 poslužitelja, zaražene web stranice na kojoj je udomljen zlonamjerni sadržaj i sl.
(O2)	Prikupljanje informacija			Prijave u kojima nije detektiran pokušaj napada, već skeniranje IP adresa/priključaka (eng. *port*) i sl., enumeracija ili slična aktivnost prikupljanja tehničkih podataka koji bi bili korisni za provođenje kibernetičkog napada.
(O3)	Pokušaj neovlaštenog pristupa	(O31)	Pogađanje pristupnih podataka	Pokušaj napada kroz pogađanje zaporki (eng. *bruteforce*, *password spray* i sl. aktivnosti) ili druge vrste pristupnih podataka. Ovo obuhvaća incidente u kojima pogađanje nije bilo uspješno, ali i one u kojima je bilo uspješno na način da je npr. uspješno kompromitiran jedan ili više računa e-pošte, ali to nije dovelo do šire ugroze informacijskog sustava.
		(O32)	Pokušaj iskorištavanja ranjivosti	Pokušaj napada kroz iskorištavanje ranjivosti. Obuhvaća incidente gdje iskorištavanje nije bilo uspješno ili je tehnički samo iskorištavanje bilo uspješno, ali nije imalo gotovo nikakav utjecaj.
(O4)	Uspješno ostvarena kompromitacija	(O41)	Ucjenjivački napad	Obuhvaća *ransomware* napade i druge vrste ucjenjivačkih kibernetičkih napada u kojima je kompromitiran informacijski sustav te se traži plaćanje otkupnine kako bi se otključao/vratio pristup informacijskom sustavu, kako ne bi bili objavljeni ukradeni podaci, kako se ne bi uskratila dostupnost i sl. Obuhvaća i napade u kojima se dogodila kompromitacija informacijskog sustava te

				je izgledno da se radilo o pokušaju ucjenjivačkog napada, ali je napad zaustavljen na vrijeme (npr. prije zaključavanja i/ili krađe podataka).
		(O42)	Krađa pristupnih podataka	Incidenti u kojima su ukradeni pristupni podaci (lozinke, HTTP kolačići i sl.), npr. kroz zarazu jednog ili više uređaja krajnjih korisnika s *infostealer* zlonamjernim kodom.
		(O43)	Krađa podataka	Incidenti kojima je glavna karakteristika krađa podataka, uobičajeno veće količine podataka poput baza podataka s osobnim podacima ili drugim osjetljivim podacima. Krađa podataka može primjerice biti izvršena kroz kompromitaciju informacijskog sustava, kroz neovlašteno automatizirano prikupljanje podataka s javno dostupnih sučelja (eng. *scraping*) ili kroz unutarnju prijetnju, tj. neovlašteno dijeljenje podataka koje je proveo zaposlenik subjekta.
		(O44)	Neovlaštena izmjena sadržaja	Incidenti kojima je glavna karakteristika neovlaštena izmjena sadržaja poput kompromitacije s ciljem izmjene sadržaja (npr. *web defacement*).
		(O45)	Kompromitacija s uništavajućim učinkom	Napadi čiji je krajnji cilj bio uništavajući, tj. kojem je cilj onesposobiti IT ili OT sustav ili mu narušiti integritet s ciljem stvaranja štete (npr. brisanje/prepisivanje podataka i konfiguracije ili mijenjanje parametara do nesigurnih razina).
		(O46)	Kompromitiran uređaj	Incidenti koji ne pripadaju drugim potkategorijama, a kojima je glavna karakteristika kompromitacija jednog uređaja (npr. računalo zaraženo kroz preuzimanje i instalaciju), ili kompromitacija više uređaja, ali bez lateralnog

				širenja zaraze odnosno bez ugroze za širi informacijski sustav.
		(O47)	Kompromitiran informacijski sustav	Incidenti koji ne pripadaju drugim potkategorijama, a u kojima je kompromitiran informacijski sustav, odnosno u kojima je kompromitacija obuhvatila više komponenti informacijskog sustava. Primjerice, uspješno pogađanje zaporki za VPN pristup, nakon čega je napadač pristupio unutarnjoj mreži te pristupao unutarnjim resursima, kompromitirao druge korisničke račune ili uređaje i sl.
(O5)	Nedostupnost usluge	(O51)	Uskraćivanje usluge	Nedostupnost usluge koja je rezultat napada odnosno neke zlonamjerne radnje, poput DoS/DDoS napada. Nedostupnost je privremene naravi (npr. dok aktivno traje napad), a ne trajna.
		(O52)	Ispad usluge	Nedostupnost usluge za koju nema indikacije da je rezultat napada odnosno zlonamjerne radnje, već je rezultat greške, nesreće ili prirodne nepogode.
(O6)	Prijevare	(O61)	*Phishing* napad	Pokušaj navođenja korisnika na odavanje povjerljivih podataka ili pokretanje zlonamjernog koda putem raznih komunikacijskih kanala (najčešće elektroničke pošte). *Phishing* napadi (i *credential phishing* i *phishing* napadi sa zlonamjernim kodom) i druge prijevare tehničke naravi. Ako je *phishing* bio početak napada koji je imao veći utjecaj, npr. rezultirao je kompromitacijom cijelog informacijskog sustava i ucjenjivačkim napadom, onda se radi o drugom odgovarajućem operativnom učinku.
		(O62)	Poslovne prijevare	Prijevare kod kojih napadač lažnim predstavljanjem pokušava

				steći ili stekne financijsku korist od poslovnog subjekta. Neki od najčešćih oblika ovakvih napada su tzv. „*CEO fraud*“ ili „*BEC*“ (*Business Email Compromise*).
		(O63)	Ostale vrste financijski motiviranih prijevara	Ostale prijevare kod kojih napadač pokušava steći ili stekne financijsku korist.
(O7)	Neželjene poruke			Podrazumijeva neželjenu elektroničku poruku reklamnog ili neistinitog sadržaja, najčešće s ciljem reklamiranja proizvoda, zastrašivanja ili dezinformiranja primatelja.
(O8)	Ostalo			Podrazumijeva neželjene događaje koji ne mogu biti opisani ranije navedenim atributima, a koji bi se mogli okarakterizirati kao kibernetički 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 se pojašnjavaju kriteriji 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.
(U6)	Bez utjecaja	Nije bilo utjecaja na osnovna načela informacijske sigurnosti.

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 dugotrajnu prisutnost u kompromitiranom sustavu uz aktivirane sposobnosti sprječavanja detekcije.
(D6)	Nepoznato	Nije moguće odrediti fazu napada.

Mogućnosti daljnje razrade i primjene u budućnosti

Nacionalnu taksonomiju je potrebno koristiti kao alat koji će omogućiti efikasnu razmjenu informacija u svrhu bržeg uočavanja i sprječavanja kibernetičkih incidenata. Nacionalna taksonomija:

1. Omogućava brzu identifikaciju i opis kibernetičkog 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 se izrada 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 se 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, 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 kibernetičkog incidenta. Također, moguće je provesti i integraciju sa sustavom klasifikacije incidenata/događaja *Traffic Light Protocol* (*TLP*[3]). *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 prikupljeno znanje te odmah po prijavi događaja ili incidenta donositi određene zaključke o akterima, strategiji obrane i utjecaju na cjelokupnu razinu sigurnosti.

[3] *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/

Prilog 1 – Identifikacija poznatih kibernetičkih incidenata primjenom atributa Operativni učinak

Tip ugroze	Vrijednost	Potkategorija
Ransomware – šifriranje podataka	Uspješno ostvarena kompromitacija	Ucjenjivački napad
Web Defacement	Uspješno ostvarena kompromitacija	Neovlaštena izmjena sadržaja
Skeniranje mreže *Nmap* alatom	Prikupljanje informacija	Nema potkategorije
Phishing stranica na domeni registriranoj u zlonamjerne svrhe	Napadačka infrastruktura	Nema potkategorije
Zeus upravljački poslužitelj	Napadačka infrastruktura	Nema potkategorije
Phishing kampanja	Prijevare	*Phishing* napad
Spam kampanja	Neželjene poruke	Nema potkategorije
Kompromitiran *Gmail* račun	Uspješno ostvarena kompromitacija	Krađa pristupnih podataka
SYN flood	Nedostupnost usluge	Uskraćivanje usluge
Brute force	Pokušaj neovlaštenog pristupa	Pogađanje pristupnih podataka
Mirai bot	Uspješno ostvarena kompromitacija	Kompromitiran uređaj

Prilog 2 – Identifikacija poznatih kibernetičkih 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)	Uspješno ostvarena kompromitacija/Kompromitiran uređaj (4/6)	Otkrivanje (4)	Korisnik (4)	Kompromitacija (4)

V5_O46_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)	Uspješno ostvarena kompromitacija/Ucjenjivački napad (4/1)	Uništenje (3)	Lokalno računalo (3)	Kompromitacija (4)

V5_O41_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)	Uspješno ostvarena kompromitacija/Ucjenjivački napad (4/1)	Prekid (2)	Upravljačka infrastruktura (1)	Kompromitacija (4)

V5_O41_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)	Uspješno ostvarena kompromitacija/ Neovlaštena izmjena sadržaja (41/4)	Iskrivljavanje (1)	Aplikacijski sustav (5)	Kompromitacija (4)

V2_O44_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/(2)	Otkrivanje (4)	Računalna mreža (2)	Izviđanje (1)

V3_O2_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)	Nedostupnost usluge/ Uskraćivanje usluge (5/1)	Prekid (2)	Računalna mreža (2)	Kompromitacija (4)

V3_O51_U2_N2_D4

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

Primjer – Tijek *Agent Tesla* 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)	Uspješno ostvarena kompromitacija/Kompromitirani uređaj (4/6)	Otkrivanje (4)	Korisničko računalo (3)	Kompromitacija (4)

V5_O46_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)	Uspješno ostvarena kompromitacija/Kompromitiran informacijski sustav (4/7)	Otkrivanje (4)	Upravljačka infrastruktura (1)	Kompromitacija (4)

V5_O47_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 V5_O4_U4_**N3**_D4

Strategija obrane: Ukloniti kompromitirano računalo s mreže

Faza 2 V5_O4_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.

Sigurnosno-obavještajna agencija

Nacionalni centar za kibernetičku sigurnost

Savska cesta 39/1, 10000 Zagreb

Republika Hrvatska

Kontakt:

E-mail: info@ncsc.hr

www.ncsc.hr

Hrvatska akademska i istraživačka mreža - CARNET

Sektor Nacionalni CERT

Josipa Marohnića 5, 10000 Zagreb

Republika Hrvatska

Kontakt:

E-mail: ncert@cert.hr

www.cert.hr