SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

ZAVRŠNI RAD br. 1075

Određivanje ekonomske štete u organizaciji nastale kao posljedica kibernetičkog napada

Nina Sokol

Zagreb, lipanj 2023.

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

ZAVRŠNI RAD br. 1075

Određivanje ekonomske štete u organizaciji nastale kao posljedica kibernetičkog napada

Nina Sokol

Zagreb, lipanj 2023.

SVEUČILIŠTE U ZAGREBU

FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Zagreb, 10. ožujka 2023.

ZAVRŠNI ZADATAK br. 1075

Pristupnica: **Nina Sokol (0036531788)**

Studij: Elektrotehnika i informacijska tehnologija i Računarstvo

Modul: Računarstvo

Mentor: izv. prof. dr. sc. Stjepan Groš

Zadatak: **Određivanje ekonomske štete u organizaciji nastale kao posljedica kibernetičkog napada**

Opis zadatka:

Tijekom i nakon kibernetičkog napada na neku organizaciju generiraju se ekonomske štete. Dosta je teško odrediti točan iznos gubitka te se često štete paušalno procjenjuju. Međutim, postoji mogućnost preciznijeg određivanja štete korištenjem simulatora CCS gdje simulator simulira napad i obranu i tijekom te simulacije izračunava kolika je šteta. U sklopu završnog rada potrebno je uzeti model neke generičke organizacije te u toj organizaciji definirati što je moguće više mjesta na kojima nastaje šteta. Kako bi se odredili mogući izvori štete treba koristiti javno dostupne izvore koji se bave s tom temom. Te izvore štete potrebno je ugraditi u model organizacije nad kojim se potom simulira napad i obrana korištenjem simulatora CCS. Dodatno, treba pokušati varirati izvore šteta i koliko doprinosi svaki izvor ukupnoj šteti te odrediti na koje su parametre konačna šteta najosjetljivija. Citirati korištenu literaturu i navesti dobivenu pomoć.

Rok za predaju rada: 9. lipnja 2023

Sadržaj

1. Uvod

Kibernetički napadi na organizacije događaju se svakodnevno. Organizacijama je obično potrebno nekoliko mjeseci da otkriju sigurnosni incident nakon čega se trude što prije riješiti problem [6]. Često ne postoje planovi za rješavanje incidenata pa se zbog toga niti ne bilježi ekonomska šteta koja nastaje tijekom i nakon kibernetičkog napada. Ona se pokušava procijeniti nakon što je incident riješen, no teško se naknadno sjetiti koji faktori i u kolikoj mjeri utječu na ukupnu štetu. Zato je šteta koja se objavljuje u medijima najčešće samo gruba procjena stvarne štete.

Osim napadnute organizacije, točan iznos ekonomske štete koja je rezultat kibernetičkog napada zanima i banke te osiguravajuća društva. Bankama je potrebna informacija kakav utjecaj ekonomska šteta ima na kreditnu sposobnost organizacije, odnosno njezinu mogućnost da u zadanom roku otplati kredit [1]. Osiguravajuća društva trebaju procijeniti rizik od ponovnog napada kako bi prilagodila premiju osiguranja za organizaciju te odrediti koji dio štete polica osiguranja pokriva ako je organizacija bila unaprijed osigurana protiv kibernetičkog napada [2].

Ne postoji sustavan i pouzdan način određivanja ekonomske štete u organizaciji. Pri određivanju štete se radi procjena pomoću kalkulatora za izračun štete [2] ili tablica s popisima izvora štete koje je potrebno uzeti u obzir [3], no oni mogu biti neprecizni i međusobno neusporedivi. Za izračun štete u ovom radu je korišten simulator za uvježbavanje organizacija kako reagirati nakon pojave incidenta. *Cyber Conflict Simulator* (CCS) je nastao suradnjom Utilis d. o. o i FER-a [4], a omogućava simulaciju koraka napada i obrane te bilježenja nastale štete. Pregledom dnevnika svih akcija nakon simulacije moguće je detaljnije odrediti koji su sve izvori napada i kakvu štetu oni generiraju.

Ovaj rad daje pregled kako nastaje ekonomska šteta kao posljedica kibernetičkog napada te je opis izvora takve štete dan u drugom poglavlju. U trećem poglavlju će se detaljnije opisati CCS i kako se u njemu definira izračunavanje štete tijekom simulacije. Četvrto poglavlje prikazuje demonstraciju izračuna štete za napad u jednoj generičkoj organizaciji pomoću simulatora i analize dnevnika akcija, dok peto poglavlje donosi usporedbu koliko izračunata šteta pomoću simulatora odstupa s procjenama iznosa štete u literaturi.

2. Šteta uzrokovana kibernetičkim napadom

Svaki sustav ima propisane sigurnosne zahtjeve koji moraju biti zadovoljeni da bi se on smatrao sigurnim. Ako neki od sigurnosnih zahtjeva nije zadovoljen, u sustavu je došlo do incidenta. Kibernetički napad je aktivnost kojoj je cilj narušiti sigurnost računalnog sustava ili informacije, odnosno uzrokovati incident [5]. Najčešće se radi o napadima u kojima je cilj napadača ukrasti povjerljive i osjetljive informacije o organizaciji ili njezinim klijentima [2]. Ekonomska šteta uzrokovana kibernetičkim napadom je svaki trošak koji organizacija ima pri rješavanju incidenta, a ne spada u predviđene i očekivane troškove poslovanja te svi kratkoročni i dugoročni gubitci koje organizacija pretrpi zbog ukradene ili oštećene imovine, podataka i intelektualnog vlasništva [2, 3, 10].

Od samog napada do otkrivanja da je došlo do narušavanja sigurnosti sustava protekne u prosjeku nekoliko mjeseci [6], a posljedice napada mogu dugoročno nanositi štetu organizaciji. Zbog ovako dugog perioda koji treba uzeti u obzir pri izračunu štete i ne postojanja sistematiziranog načina izračuna štete, organizacijama je teško odrediti koliko ih je kibernetički napad zapravo koštao. Ekonomska šteta ovisi o vrsti napada koji se dogodio, industrijskom sektoru kojem organizacija pripada, državi u kojoj organizacija posluje te vremenu i okolnostima u kojima je javnost obaviještena da je došlo do incidenta u organizaciji, ali i o samim koracima koje je organizacija napravila kako bi se obranila od napada [7]. Stoga je teško uspoređivati iznose koje su organizacije objavile kao svoju procjenu ekonomske štete i odrediti koja od njih ima najtočniju metodu izračuna ukupne ekonomske štete nakon kibernetičkog napada.

2.1. Općeniti izvori štete

Izvori štete se prema tipu dijele na izravne izvore štete i neizravne izvore štete [3, 7, 9]. U literaturi ova podjela nije u potpunosti usklađena, pa postoji više različitih naziva za ove kategorije šteta. Neki autori izdvajaju troškove zaštite od daljnjih napada kao zasebnu kategoriju [10], dok ostali ove troškove pribrajaju izravnim izvorima štete. Alternativni naziv za izravne troškove su opipljivi troškovi, a za neizravne neopipljivi troškovi [8]. U dijelu literature se ne radi prvo podjela na izravne i neizravne izvore štete pa onda daljnja podjela na podtipove šteta unutar njih već se ukupna šteta dijeli na troškove gubitka

kontrole nad sustavom, troškove gubitka proizvoda, gubitak koji nastaje kada radnici ne obavljaju redovan posao, troškove oštećenja opreme, troškove prevencije daljnjih napada [11]. Još jedan način definiranja kategorija štete je podjela na troškove istrage napada, troškove obavještavanja javnosti i upravljanje kriznom situacijom, troškove sankcija regulatornih tijela te pravne troškove [2].

Troškovi se prema vremenu mogu podijeliti na kratkoročne, srednjoročne i dugoročne [3]. Kratkoročni su oni troškovi koji su nastali u vremenu otkrivanja i rješavanja napada, srednjoročni su troškovi koji su nastali u kraćem periodu nakon napada, a dugoročni troškovi mogu nastajati godinama nakon napada kao njegove posljedice.

Prilikom procjene štete za određeni napad, organizacija uzima u obzir samo relevantne izvore štete koji su specifični za njezinu vrstu djelatnosti i vrstu napada koji se dogodio.

2.1.1. Izravni izvori štete

Izravni izvori štete ili izravni troškovi su svi gubitci koji se mogu izravno povezati s rješavanjem kibernetičkog napada, a iskazuju se u izgubljenom novcu i vremenu [3, 8]. Najčešće ih je lako prepoznati i kvantificirati te oni čine najveći dio ukupne štete.

Izravni izvori štete su:

- troškovi istrage napada

  Trošak istrage napada obuhvaća sve troškove koje organizacija ima pri otkrivanju kibernetičkog napada i sprečavanju širenja napada na ostatak sustava. Obično se radi o provjeri sumnjivog dijela sustava i otkrivanju ranjivosti zbog koje se dogodio napad te pokušaju da se ranjivost ukloni. Obavještava se uprava kako bi ona mogla odlučiti o daljnjim koracima [8, 9].

- troškovi zapošljavanja vanjskih suradnika koji pomažu u rješavanju napada

  Ako organizacija nema unaprijed pripremljen plan kako reagirati u slučaju kibernetičkog napada mora unajmiti tvrtku koja će joj pomoći u rješavanju napada, odnosno kibernetički tim za brzi odgovor. Ako plan postoji, organizacija može dodatno tražiti pomoć vanjskih stručnjaka za sigurnost, administratora sustava ili drugih stručnjaka specifičnih za područje u kojoj organizaciji treba pomoć pri rješavanju napada [7, 8].

U slučaju ozbiljnijeg napada koji zahtijeva napredne usluge kao što su računalna forenzika ili reverzno inženjerstvo zbog dublje analize zloćudnog koda i namjera napadača, organizacija može unajmiti kibernetički tim za brzi odgovor (eng. *Rapid response team*) koji ima stručnjake s potrebnim vještinama za obavljanje ovakvih akcija [3, 8].

- troškovi otkupnine nakon iznuđivanja

  U nekim slučajevima napada, posebno kod napada ucjenjivačkim zloćudnim kodom, organizacija se suočava sa situacijom u kojoj njezin sustav ili podaci postaju nedostupni. Napadač koristi ovu situaciju kako bi iznudio novčana sredstva od organizacije. Ako je organizacija pristala platiti otkupninu, tada se taj trošak i troškovi nastali pregovaranjem s napadačem dodaju ukupnoj šteti od kibernetičkog napada [3].

- financijski gubitci

  Financijski gubitci nastaju kada su tijekom napada ukradena novčana sredstva organizacije ili imovina kojoj je poznata cijena, poput vrijednosnih papira i dionica [3]. Trošak koji se pribraja ukupnoj šteti je zbroj svih ukradenih financijskih sredstava.

- troškovi zbog privremene ili trajne nedostupnosti usluga i servisa

  Servisi i usluge mogu postati privremeno ili trajno nedostupni zbog akcija napadača ili ih zaposlenici po naredbi uprave mogu namjerno ugasiti ili odspojiti s mreže kako bi spriječili napadača od nanošenja dodatne štete organizaciji. Problem je u tome što kada pojedini servisi i usluge nisu dostupni, klijenti im ne mogu pristupati te organizacija ima trošak u iznosu očekivanog profita koji bi ti servisi i usluge donijeli da su bili u normalnoj funkciji [3]. S ovim izvorom štete su usko povezani i izvori štete kada zaposlenici ne mogu obavljati svoj uobičajeni posao jer ne mogu pristupiti dijelovima sustava, te šteta zbog gubitka povjerenja klijenata.

- troškovi oporavka podataka ili informacija

  Troškovi oporavka podataka ili informacija nastaju kao rezultat napada u kojem dio podataka postane nedostupan zbog krađe ili šifriranja od strane napadača. U ove troškove spada oporavak podataka iz pričuvnih kopija ili generiranje novih podataka ako pričuvne kopije nisu dostupne ili ne postoje. Primjerice, ako se radi o

korisničkim računima, oni će se resetirati te će biti potrebno pružiti pomoć klijentima pri ponovnom postavljanju računa [8].

- troškovi zbog objavljivanja ili prodaje informacija u ukradenim dokumentima

  Nakon što ukrade dokumente s privatnim ili osjetljivim podacima, napadač ih može prodati ili objaviti. Tada se organizacija suočava s troškovima koji uključuju vrijednost samih dokumenata, ali i troškovima nadzora kako bi se spriječila zloupotreba ukradenih podataka. Podatke može iskoristiti i organizacija koja je konkurencija napadnutoj organizaciji s ciljem poboljšanja svog poslovanja [8].

- troškovi gubitka kontrole nad sustavom

  Organizacije u industrijskim postrojenjima koriste sustave nadzora i upravljanja (SCADA) za upravljanje, slanje i prikupljanje podataka nekog udaljenog dijela sustava [13]. Ako ovaj sustav postane nedostupan ili mu je narušen dio funkcionalnosti u napadu, postrojenje je potrebno djelomično ili u cijelosti upravljati ručno. To znači da je potrebno prevesti potreban broj radnika na lokaciju kojom je upravljao SCADA sustav kako bi oni njime ručno upravljali što će rezultirati sporijim radom sustava nego obično [11]. Ovakav način upravljanja je neefikasan, zbog čega nastaju veći troškovi nego da se sustavom automatski upravlja.

- gubitak proizvoda

  Organizacije koje u svojoj proizvodnji koriste materijale koji su valjani samo kratki period poput hrane, mogu imati troškove zbog gubitka proizvoda ako sustav sporije radi ili ne radi uopće kao posljedica napada. Troškovi koji nastaju su smanjenje proizvodnje, trošak zbrinjavanja viška materijala koji se više ne može koristiti zbog isteka roka valjanosti, ali i rupe u proizvodnji zbog nedostupnosti dijelova proizvoda ili prevelikog čekanja na njih [11].

- troškovi nastali jer radnici ne obavljaju svoj uobičajeni posao

  Za vrijeme napada, dio zaposlenika je preusmjeren na rješavanja problema koji su nastali kao posljedica napada. Zato ne mogu istovremeno obavljati svoj uobičajeni posao te tada taj posao počinje stvarati štetu u organizaciji [3].

  Ako je sustav djelomično ili u potpunosti nedostupan, zaposlenici koji se ne bave rješavanjem napada ne mogu obavljati svoj posao, ali još uvijek primaju plaću pa je šteta koja ovdje nastaje očekivani profit koji bi organizacija imala da su zaposlenici

normalno obavljali svoj posao. Iznos plaće se ne pribraja šteti jer bi zaposlenici bili plaćeni neovisno o pojavi napada [11].

- troškovi popravka oštećene fizičke opreme

  Jedna od posljedica kibernetičkog napada može biti i oštećenje fizičke opreme, najčešće u upravljačkim sustavima. Tu opremu je potrebno ili zamijeniti ili popraviti pa se ukupnoj šteti pribraja cijena popravka ili zamjene opreme te očekivani profit koji bi organizacijama imala od opreme da je normalno radila [11].

- troškovi nadogradnje sustava

  Organizacija nakon kibernetičkog napada želi smanjiti rizik od daljnjih napada. Tijekom napada se uočavaju ranjivosti u sustavu pa organizacija ažurira i nadograđuje sustav ili u potpunosti mijenja vrstu sustava, programa i opreme koje koristi [9, 11]. Time nastaju troškovi nadogradnje sustava u koje spada cijena nove programske potpore, trošak koji nastaje kada sustav nije dostupan zbog nadogradnje te trošak smanjenja produktivnosti zaposlenika koji koriste taj sustav zbog perioda privikavanja na novo radno sučelje. Ovaj trošak se može umanjiti ako se organiziraju dodatne edukacije zaposlenika kako koristiti novi sustav, no tada te edukacije predstavljaju dodatne troškove. U ove troškove se ne bi trebali ubrajati troškovi nadogradnje sustava koja je bila planirana neovisno o kibernetičkom napadu i do koje bi došlo čak i da se napad nije dogodio [3] te bi u obzir trebalo uzeti i činjenicu da je nadogradnjom sustava olakšano sprječavanje i detekcija budućih napada pa bi se dio troškova trebao prenijeti i na njih.

- pravni troškovi

  Nakon kibernetičkog napada, organizacija mora potražiti odvjetnika ili drugu pravnu osobu koja će joj pružiti pravni savjet kako postupiti s pravnog stajališta i koga je sve dužna obavijestiti o napadu [3, 8, 9].

- kazne i naknade regulatornim tijelima

  Organizacije trebaju prijaviti napad regulatornim tijelima i kontinuirano ih izvještavati o njegovom rješavanju. Regulatorno tijelo određuje treba li organizacija platiti kazne i naknade te koliki je njihov iznos ovisno o vrsti napada koji se dogodio i tipu informacije koja je kompromitirana. Iznos kazni i naknada koje organizacija plaća regulatornim tijelima nakon napada pribraja se ukupnoj šteti [3, 8, 9].

- povećanje troškova otplate kredita

Kibernetički napad povećava rizik od novih napada, te smanjuje kreditnu sposobnost organizacije [8]. Ako je u organizaciji došlo do novčanih gubitaka zbog napada, a ona trenutno otplaćuje kredit, može doći do produljenja vremena otplate, što znači da će ukupna cijena kredita na kraju biti veća. Razlika između stvarne i očekivane ukupne cijene kredita predstavlja dodatni trošak za organizaciju. Zbog smanjenja kreditne sposobnosti, organizacija će u budućnosti imati problema s podizanjem novih kredita ili pozajmica te će joj to stvarati dodatne troškove [3].

- povećanje troškova premija osiguranja

  Nakon kibernetičkog napada povećan je rizik od ponovnih napada što u obzir uzimaju i osiguravajuća društva pri izračunu novih premija osiguranja [3, 8]. Razlika između nove i stare premije osiguranja je dodatni trošak organizaciji koji se pribraja ukupnoj šteti od napada.

- troškovi plaćanja unaprijed dogovorenog viška osiguranja

  Ako je organizacija osigurana protiv kibernetičkog napada, tada s osiguranjem ima dogovorenu svotu do koje sama pokriva troškove napada ako se on dogodi, odnosno franšizu [3]. Ukupni iznos police osiguranja koji bi osiguravajuće društvo trebalo isplatiti organizaciji umanjuje se za taj iznos.

- troškovi treniranja zaposlenika kako reagirati za vrijeme napada

  Ukupni troškovi obuhvaćaju ulaganja u treniranje zaposlenika kako bi se osigurala adekvatna reakcija tijekom napada. Troškovi koji se javljaju pri treniranju zaposlenika su troškovi tečaja ili instruktora koji treniraju zaposlenika, troškovi najma prostora i materijala potrebnih za treniranje [3] te troškovi koji nastaju jer zaposlenici ne rade svoj uobičajeni posao za vrijeme pohađanja tečaja.

- troškovi obavijesti javnosti

  Troškovi povezani s obavještavanjem klijenata i javnosti o napadu uključuju vrijeme i resurse potrebne za objavljivanje obavijesti te troškove koji nastaju kada se klijenti oštećeni u napadu moraju pojedinačno obavijestiti osobno, putem telefona ili elektroničkim putem [8].

- troškovi rada službe za korisnike vezani uz napad

  Ako su za vrijeme ili nakon napada, sustav ili podaci nedostupni klijentima, organizacija mora imati službu za korisnike koja će odgovoriti klijentima na sva

pitanja vezana uz napad te im pomoći ponovno postaviti sve usluge koje koriste ako su one postale nedostupne klijentima kao posljedica napada [7]. Troškovi prekovremenog rada službe za korisnike vezano uz napad ili zapošljavanje dodatnog osoblja kako bi se mogla obraditi količina upita vezana uz napad dodaju se ukupnoj šteti.

- popusti i kompenzacije klijentima koji su pretrpjeli štetu zbog napada

  Organizacija pokušava zadržati povjerenje klijenata koji su oštećeni u kibernetičkom napadu pa ih kompenzira za podatke koje su izgubili ili im nudi popuste i posebne pogodnosti s ciljem smanjenja daljnjih troškova koje bi imala da izgubi te klijente ili da nastanu pravni sporovi s tim klijentima [3, 8]. Iznos kompenzacija plaćenih klijentima i popusta danog klijentima predstavlja trošak za organizaciju.

2.1.2. Neizravni izvori štete

Neizravni izvori štete ili neizravni troškovi su svi gubitci koji nisu direktno povezani s napadom već nastaju kao njegova posljedica. Povezani su s emocijama i stavom klijenata, zaposlenika, javnosti i poslovnih partnera prema organizaciji te izgubljenim intelektualnim vlasništvom i narušenim samopouzdanjem organizacije umjesto s izravnim novčanim troškovima [3]. Teško ih je odrediti i kvantificirati jer se ovi troškovi smatraju još i reputacijskim troškovima. Reputacijski troškovi su gubitci koji nastaju u organizaciji zbog narušene reputacije i ugleda organizacije te gubitka povjerenja njezinih klijenata. Literatura nije dosljedna u tome koji točno izvori spadaju u kategoriju neizravnih izvora štete. Neki većinom zanemaruju ove izvore štete [8], dok oni koji ih prepoznaju ponekad dio neizravnih izvora štete svrstavaju u kategoriju izravnih izvora štete [3, 7, 9].

Neizravni izvori štete su:

- troškovi zbog izgubljenog intelektualnog vlasništva

  Intelektualno vlasništvo su svi dokumenti, patenti, poslovna pravila i načini poslovanja u kojima se organizacija razlikuje od svoje konkurencije [14]. Kada su takvi podaci ukradeni tijekom napada, organizacija trpi štetu u visini profita koje je trebala ostvariti da intelektualno vlasništvo nije ukradeno ili objavljeno [3]. Budući da je vrlo teško procijeniti kolika je novčana vrijednost intelektualnog vlasništva, ovaj izvor štete spada u neizravne izvore.

- propuštene prilike

  Organizacija može pretrpjeti štetu ako zbog narušene reputacije nakon objave da je pretrpjela napad ne uspije ostvariti suradnju s drugim organizacijama ili privući nove klijente [2]. Nakon napada, samopouzdanje organizacije je narušeno pa je moguće da će propustiti prilike za ostvarivanje profita [8] jer se neće uključiti u prijave na natječaje ili subvencioniranje zbog straha od novih napada i slike organizacije u medijima.

- problemi s lancem opskrbe

  Problemi s lancem opskrbe mogu nastati ako organizacija zbog prekida poslovanja ili njegovog sporijeg rada ne može isporučiti dio proizvoda na vrijeme te onda za njih ne dobiva očekivanu naknadu, a ima i dodatne troškove za zbrinjavanje i skladištenje tih proizvoda [12]. S druge strane, organizacija može pretrpjeti gubitke ako zbog narušenog ugleda nakon kibernetičkog napada druge organizacije koje sudjeluju u lancu opskrbe odbiju raditi s njom [3]. Tada opet ima troškove za zbrinjavanje proizvoda koje ima, ali i troškove zbog usporenog ili prekinutog poslovanja dok lanac opskrbe nije u normalnoj funkciji.

- troškovi pada cijena dionica

  Nakon objave da je došlo do kibernetičkog napada javnosti, organizacija može očekivati da će joj cijene dionica pasti. Ovo je neizravni izvor štete jer na rast ili pad cijene dionice ne utječe samo reputacija koju organizacija ima u javnosti, već i niz drugih faktora, poput industrijskog sektora u kojem posluje te općenitog stanja i prilika na tržištu u vrijeme objave da je došlo do incidenta. Zbog toga, neke organizacije bilježe nagli pad cijena dionice u danima nakon obavijesti o napadu, ali se cijena dionica brzo oporavlja, dok druge organizacije doživljavaju dugotrajne posljedice smanjenja vrijednosti dionica [9].

- gubitak ulagača i financiranja

  Kada organizacija pretrpi napad, dolazi do povećanja rizika od novih napada pa ulagači mogu povući svoju potporu ili tražiti veće naknade zbog povećanog rizika što predstavlja dodatne troškove organizaciji [9]. Iz istog razloga može izgubiti i druge izvore financiranja ako se donatori žele udaljiti od organizacije zbog negativne reputacije u medijima [3].

- ugled organizacije u medijima

Obavijest da je došlo do kibernetičkog napada u organizaciji za sobom povlači negativni utjecaj na ugled organizacije zbog čega organizacija ne dobiva nove klijente [3]. Trošak koji time nastaje je očekivani profit koji je organizacija trebala ostvariti od novih klijenata.

- gubitak povjerenja klijenata

  Klijenti gube povjerenje u organizaciju, pogotovo ako je tijekom napada došlo do narušavanja povjerljivosti njihovih privatnih podataka, pa prestaju poslovati s njom ili to rade u mnogo manjoj mjeri nego ranije zbog čega organizacija trpi gubitke čiji je iznos teško procijeniti [3, 7, 8].

- gubitak povjerenja zaposlenika

  Zaposlenici mogu izgubiti povjerenje u organizaciju u kojoj rade zbog povećanog rizika od daljnjih napada te ako odluče promijeniti posao, organizacija ima trošak zapošljavanja i treniranja novih zaposlenika za njihovo radno mjesto [8].

- povećanje troškova zapošljavanja

  Budući da organizacija ima lošu reputaciju nakon napada i povećani rizik od daljnjih napada, dolazi do povećanja troškova zapošljavanja jer zaposlenici traže dodatne kompenzacije zbog povećane nesigurnosti na radnom mjestu [3].

- smanjenje produktivnosti na radnom mjestu

  Kibernetički napad ima emocionalni i fizički utjecaj na zaposlenika zbog čega je on slabije koncentriran na radnom mjestu te zadatke obavlja sporije [8] ili je pod stresom zbog skraćenih rokova za izvršavanje zadataka jer se želi što prije nadoknaditi zaostatak koji je nastao u poslu tijekom napada. Može doći i do smanjenja produktivnosti u području istraživanja jer se odbija preuzeti nepotrebne rizike [3]. Svi ovi faktori utječu na povećanje troškova poslovanja organizacije jer se posao obavlja sporije nego inače.

- pravni sporovi s oštećenim klijentima

  U slučaju pravnih sporova podignutih od strane klijenata protiv organizacije ili njezinih zaposlenika vezano uz kibernetički napad [3, 8], troškovi povezani s tim sporovima, uključujući angažiranje odvjetnika i vrijeme zaposlenika utrošeno na njih umjesto na redovne poslovne aktivnosti, predstavljaju neizravne izvore štete koji nisu mogli biti unaprijed predviđeni i kvantificirani.

- povećani rizik od daljnjih napada

  Organizacija nakon kibernetičkog napada ima povećani rizik da će ponovno biti meta istog ili sličnih napada [8], stoga je potrebno napraviti analizu rizika u organizaciji koja je dodatni trošak za organizaciju.

2.2. Variranje izvora štete

Pri izračunu ekonomske štete mogu se varirati metode za izračun štete ovisno o dostupnim podacima te vrsti napada i odgovora na napad koji se dogodio. Također, različite organizacije će izvore štete iz poglavlja 2.1 prilagoditi svojem načinu poslovanja pa će i u tom pogledu postojati razlike u izračunu ukupne ekonomske štete nakon kibernetičkog napada.

Jedna od metoda izračuna štete je predložena u [8]. Temelji se na određivanju svih izvora štete koji su primjenjivi na kibernetički napad koji se dogodio u organizaciji. Kako bi se izračunala šteta, potrebno je za svaki od izvora štete odrediti koliko je zaposlenika bilo uključeno u rješavanje tog aspekta napada te koliko im je ukupno sati bilo za to potrebno. Šteta za jednog zaposlenika se računa kao ukupan broj sati koje je utrošio na radnje povezane s rješavanjem incidenta ili njegovih posljedica u organizaciji pomnožen s cijenom jednog sata rada tog zaposlenika. Ukupna šteta se dobije zbrajanjem šteta za sve zaposlenike koji su bili uključeni u rješavanje napada ili njegovih posljedica. Nedostatak ove metode je što ne pribraja troškove poput direktnih novčanih gubitaka od krađe dokumenata, sudskih sporova i krađe novčanih sredstava tijekom napada. Također, kod neizravnih izvora štete se uglavnom ne može šteta poistovjetiti s utrošenim vremenom pojedinog zaposlenika jer se radi o apstraktnim izvorima šteta.

Kod kibernetičkog napada u industrijskim postrojenjima može doći do nedostupnosti određenog dijela strojeva u postrojenju, pa [11] predlaže da se pri izračunu štete u obzir uzme postotak strojeva u postrojenju van funkcije. Štetu računa na temelju gubitaka u organizaciji kada je 25%, 50%, 75% i 100% strojeva izvan funkcije, te srednju vrijednost tih gubitaka množi s vjerojatnosti da se dogodi određena vrsta napada. U ukupnu štetu još ulaze i gubitci organizacije zbog ručnog upravljanja strojevima, troškovi popravka i zamjene strojeva, troškovi prevencije daljnjih napada i gubitak koji je organizacija pretrpjela kada zaposlenici nisu mogli upravljati dijelom sustava u kojem su bili oštećeni

strojevi. Kod ove metode je također nedostatak to što ne uzima u obzir neizravne izvore štete.

Pri izračunu ukupne ekonomske štete u organizaciji trebala bi se kombinirati oba pristupa načinu izračuna štete jer je prvi pogodniji kada su neki posao obavljali zaposlenici, dok je drugi pogodniji za industrijska postrojenja. Uz ta dva pristupa, ukupnoj šteti bi se još trebali dodati i troškovi ostalih izvora šteta opisanih u poglavlju 2.1 budući da način izračuna i izvori štete uzeti u obzir ovise o tipu organizacije i vrsti napada koji se dogodio.

Varijacije u načinima izračuna postoje i za pojedine izvore štete. Troškovi zapošljavanja vanjskih suradnika koji pomažu u rješavanju napada ovise o tome ima li organizacija već ugovore s tvrtkama od kojih traži pomoć ili ne. Ako organizacija ima ugovor s timovima za brzi odgovor na incident, u štetu od napada neće ulaziti trošak koji organizacija ima na temelju tog ugovora osim ako u ugovoru nije drugačije definirano. Primjerice, dio troškova je fiksan neovisno o tome je li došlo do incidenta, a dio troškova snosi organizacija ako dođe do incidenta, ali je on u tom slučaju puno manji nego da ugovor uopće nije postojao. S druge strane, ako organizacija mora unajmiti tim za brzi odgovor na napad bez da je prije sklopila ugovor s tom tvrtkom, to će se smatrati troškom povezanim uz napad. Slično se mogu promatrati i troškovi za druge vanjske suradnike poput tvrtki za odnose s javnošću koje organizacija unajmljuje kao pomoć pri obavještavanju javnosti da je došlo do napada.

Troškovi obuke zaposlenika u svrhu odgovora na kibernetički napad mogu varirati ovisno o pristupu koji organizacija odabere. Ona može odlučiti kupiti *online* tečajeve za svoje zaposlenike ili angažirati usluge specijaliziranih tvrtki za obuku zaposlenika. Ovisno o veličini organizacije, tipu zaposlenika koji se trenira i duljini tečaja troškovi će varirati [15]. Na sličan način se razmatraju varijacije u troškovima edukacije zaposlenika nakon nadogradnje sustava. Troškovi će varirati ovisno o tome hoće li edukaciju održati zaposlenik organizacije, unajmljeni edukator ili će organizacija kupiti *online* tečaj za svoje zaposlenike.

Kada zaposlenici obavljaju posao vezan uz rješavanje napada i njegove posljedice, njihov uobičajen posao se ne obavlja očekivanim tempom. Ovisno o vrsti posla koji zaposlenik obavlja i on nakon nekog vremena može početi generirati štetu organizaciji koja će se pribrojiti ukupnoj šteti od napada. Visina troška ovisi o tome hoće li uobičajeni posao uopće početi generirati štetu nakon nekog vremena i ako hoće, koliki je period u kojem neće nastajati dodatna šteta.

Troškovi povezani s osiguravajućim društvima također mogu varirati ovisno o tome ima li organizacija unaprijed sklopljenu policu osiguranja i samo je želi produžiti nakon napada ili je sklapa prvi put s osiguravajućim društvom budući da će nakon napada doći do povećanja rizika od novih napada u organizaciji. Na sličan način će troškovi varirati i kada su u pitanju banke. Organizacija će imati drugačije troškove ako trenutno otplaćuje kredit, pa će zbog napada morati produljiti vrijeme otplate kredita ili nakon napada želi podići kredit u banci, a zbog povećanog rizika od ponovnih napada joj se kreditna sposobnost smanjila [3].

3. *Cyber Conflict Simulator*

Cyber Conflict Simulator (CCS) je simulator kibernetičkih napada koji omogućuje simulaciju koraka napada i obrane te prikazuje posljedice izvođenja svake akcije [16]. Simulacija se izvodi na unaprijed pripremljenom scenariju koji se sastoji od topologije te branitelja i napadača [17]. Topologija se sastoji od objekata koji mogu biti računala, mrežna oprema, programska podrška, ali i osoblje kojim organizacija raspolaže. Moguće je definirati i poslovne procese i usluge koje organizacija nudi te postaviti kontrole koje simuliraju vrstu zaštite i otpornosti objekta na napad [18]. Time je moguće detaljno prikazati strukturu organizacije koja se simulira te odrediti kako će problemi u jednom dijelu sustava utjecati na ostatak organizacije i kakva će šteta zbog toga nastati.

CCS se sastoji od *Simulatora* i *Editora*. Simulacija se izvodi u *Simulatoru* koji različitim igračima omogućava da upravljaju svojim dijelom topologije i provode akcije koje bi se provodile u stvarnosti da je došlo do napada te tako uvježbavaju svoj odgovor na napad. *Editor* služi za izgradnju topologije koja vjerno prikazuje stvarnu organizaciju. Svaki objekt ima niz atributa koje je moguće podesiti kako bi simulator što točnije simulirao njihovo ponašanje. Primjerice, objekt koji predstavlja računalo ima atribute koji opisuju kojoj organizaciji i poslovnoj jedinici pripada, na kojoj fizičkoj lokaciji se nalazi, je li uključeno i dostupno te podatke o programskoj podršci, protokolima i kontrolama koje ima implementirane. U *Editoru* se definira i način izračuna ekonomske štete u organizaciji definiranjem formula prema kojima će se šteta izračunavati te objekata u koje će se ta šteta spremati.

3.1. Izračun ekonomske štete u CCS-u

Akcije napada i obrane koje igrači pokreću tijekom simulacije utječu na promjenu iznosa ekonomske štete koja se generira tijekom napada. Šteta se u *Simulatoru* automatski računa na temelju formula definiranih u *Editoru* za zadani scenarij. Igrači tijekom simulacije mogu vidjeti kolika je šteta koja se generirala klikom na označenu ikonu u statusnoj traci na vrhu zaslona (Slika 3.1).

Slika 3.1 Statusna traka na vrhu zaslona igrača

Uobičajeno se igračima neće prikazivati dio ili čak sva generirana šteta za vrijeme simulacije. Prvi razlog je taj da pojedini igrač ne upravlja dijelom topologije u kojem nastaje šteta. Svaki igrač vidi samo onaj dio topologije kojim upravlja za vrijeme simulacije. Drugi razlog je to što generiranje štete može biti pokazatelj igračima da je došlo do narušavanja sigurnosnih zahtjeva u sustavu. To u stvarnosti nije slučaj jer se šteta obračunava tek nakon što je incident riješen. Kada bi se šteta prikazivala u simulatoru prije nego je igrač svjestan da je došlo do incidenta to bi mu bio jedan od pokazatelja da postoji problem u sustavu kojeg za vrijeme stvarnog incidenta nema.

Pregled ukupne štete generirane tijekom simulacije se može napraviti preuzimanjem dnevnika zapisa s tijekom izvođenja simulacije odabirom opcija *Settings* > *Download Scenario Review*. Preuzima se tablica s dva lista. Prvi list *Chronology* sadrži dnevnik zapisa sa svim akcijama i porukama koje su igrači napravili tijekom simulacije. Pri izračunu šteta najvažniji su zapisi tipa *Action* koji prikazuju detalje svake od provedenih akcija. Ti zapisi daju informaciju o imenu i trajanju akcije, igraču koji je akciju napravio te kojeg aktera u simulaciji je odabrao za izvršavanje akcije i s kojim parametrima (Slika 3.2).

Type	Beginning	Name / Sender	Ending / Title	Actor / Receiver	Player	Parameters / Message
Action	9.7.2022 0:45	Malware Scan	9.7.2022 0:55	IT Log&Backup Admin 01 (senior)	Incident Manager	**Actor:** IT Log&Backup Admin 01 (senior) **Target:** BISPC02 **Mode:** Delete malware

Slika 3.2 Primjer zapisa akcija u dnevniku zapisa

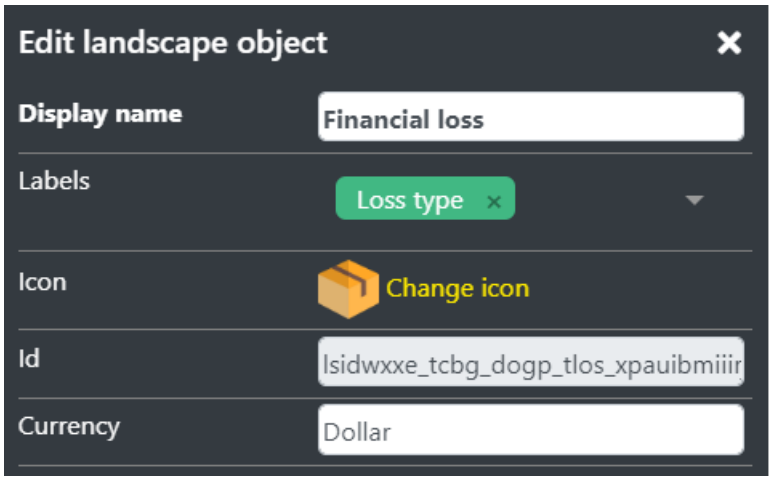
Drugi list *Indicators* daje informacije o promjeni određenih parametra unutar simulacije. Za promatranje ekonomske štete važni su stupci koji u svom nazivu sadrže *Loss* jer oni prikazuju kako se šteta povećavala tijekom simulacije u određenim dijelovima organizacije (Slika 3.3).

Time/Data	Financial Loss - Key Account Losses (€)	Financial Loss (€)	Financial Loss - Other	Financial Loss - IT (€)	Financial Loss - NDC (€)	Financial Loss - Grid imbalance (€)
10.07 00:30	0			25667	38370	
10.07 01:00	0			26862	39651	
10.07 01:30	0			26862	39651	
10.07 02:00	140000			26862	39651	
10.07 02:30	195953			26862	39651	
10.07 03:00	335907			26862	39651	

Slika 3.3 Primjer prikaza štete u dnevniku zapisa

3.1.1. Načini izračuna štete u CCS-u

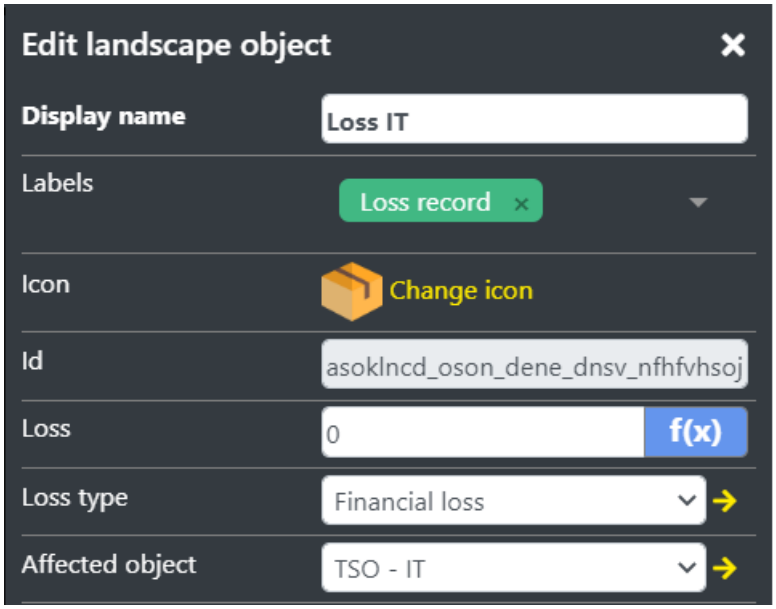
U *Editoru* se definiraju objekti u koje se sprema izračunata šteta. Najprije je potrebno definirati vrstu gubitka. Ekonomska šteta će biti definirana financijskim gubitkom u dolarima stvaranjem objekta *Financial loss* s oznakom *Loss type* (Slika 3.4).



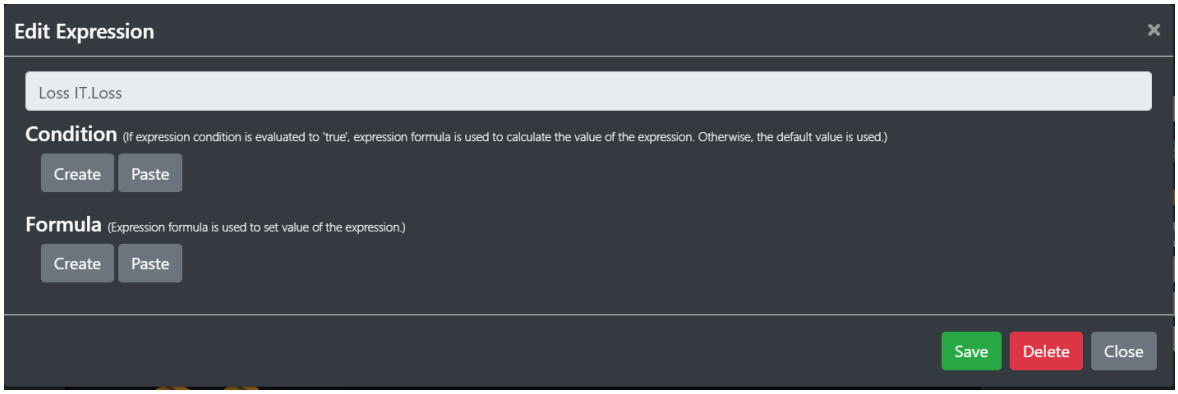
Slika 3.4 Vrsta gubitka koji se računa

Nakon što je definirana vrsta gubitka koja će se izračunavati tijekom simulacije, potrebno je napraviti objekte u koje će se izračunata šteta spremati. To će biti objekti s oznakom *Loss record* te će im kao tip gubitka biti pridružen prethodno definirani *Financial Loss.* Uz to, potrebno je svaki od objekata u koje se sprema izračunata šteta pridružiti poslovnoj jedinici za koju se ta šteta izračunava. Objekt prikazan na slici Slika 3.5 pridružen je poslovnoj jedinici *TSO – IT.* Formula za izračun štete za definirani objekt upisuje se u atribut *Loss* klikom na gumb *f(x).* Otvara se prozor kao na slici Slika 3.6. U tom prozoru je moguće postaviti uvjet (*Condition*) ako je potrebno koristiti formulu za izračun štete samo nakon zadovoljenja određenih uvjeta. Ako se uvjet ne unese, formula će se koristiti za izračunavanje štete tijekom cijele simulacije. Sama formula za izračun štete u poslovnoj jedinici kojoj definirani objekt pripada upisuje se u polje *Formula* klikom na gumb *Create* ili *Edit* ovisno o tome postoji li već definiran dio formule ili ne. Nakon odabira gumba *Create* otvara se prozor za upis formule kao na slici Slika 3.7. Formula može sadržavati objekte (engl. *Objects*), izraze (engl. *Expression*), osnovne računske operacije (engl. *Operation*), konstante (engl. *Constant*), te okrugle zagrade. Klikom na gumb *Objects* u formulu dodaje se objekt ili vrijednost nekog njegovog atributa. Klik na gumb *Expression* otvara padajući izbornik iz kojeg se može odabrati funkcija koja će se koristiti pri izračunu štete. Za izračun ekonomske štete su najvažnije funkcije *PathExists, IsAvailableFor, Accumulator, TotalOrganizationLoss, Iif.* Funkcija *PathExists* provjerava jesu li dva čvora

u mreži međusobno povezana, odnosno postoji li mrežna povezanost između ta dva čvora. Funkcija vraća *boolean.* Funkcija *IsAvailableFor* služi za provjeru je li odabrana datoteka dostupna organizaciji i ima li organizacija kriptografski ključ za dešifriranje njezinog sadržaja. Funkcija *Accumulator* zbraja gubitak kroz vrijeme u odabranu varijablu. Za zbrajanje svih gubitaka koji su povezani s organizacijom služi funkcija *TotalOrganizationLoss*, dok funkcija *Iif (Inline if)* predstavlja uvjetno grananje.

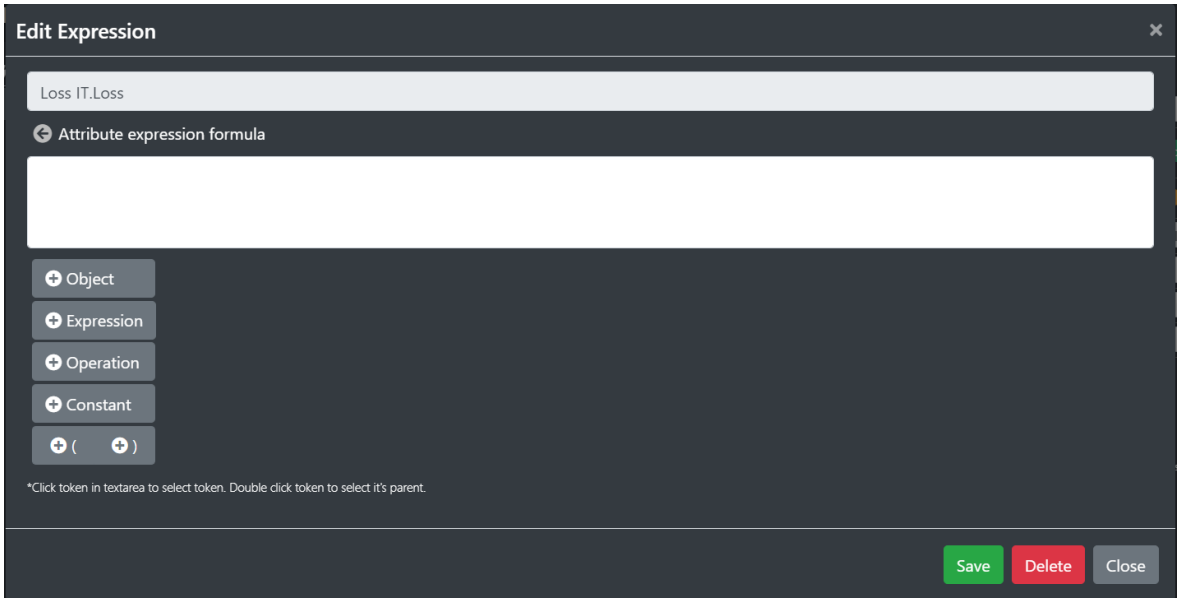


Slika 3.5 Zapis o gubitku u organizaciji



Slika 3.6 Primjer zadavanja formule za objekt tipa *Loss Record*

Primjer formule koja se može upisati je formula (1) koja provjerava je li računalo povezano na lokalnu mrežu s funkcijom *PathExists*, te ako nije, organizacija ima gubitak od 5000 $ po satu. Budući da se u simulatoru gubitak u vremenu računa po sekundi, 5000 $ po satu treba pretvoriti u gubitak od 1.388889 $ po sekundi, a gubitak kroz vrijeme se zbraja funkcijom *Accumulator* u atribut *Loss* objekta *Loss IT*.



Slika 3.7 Prozor za upis formule

$$\text{Accumulator (Loss IT. Loss, (1 – PathExists (SKAPC01, LAN SKA, time)) * 1.3888889, time)} \quad (1)$$

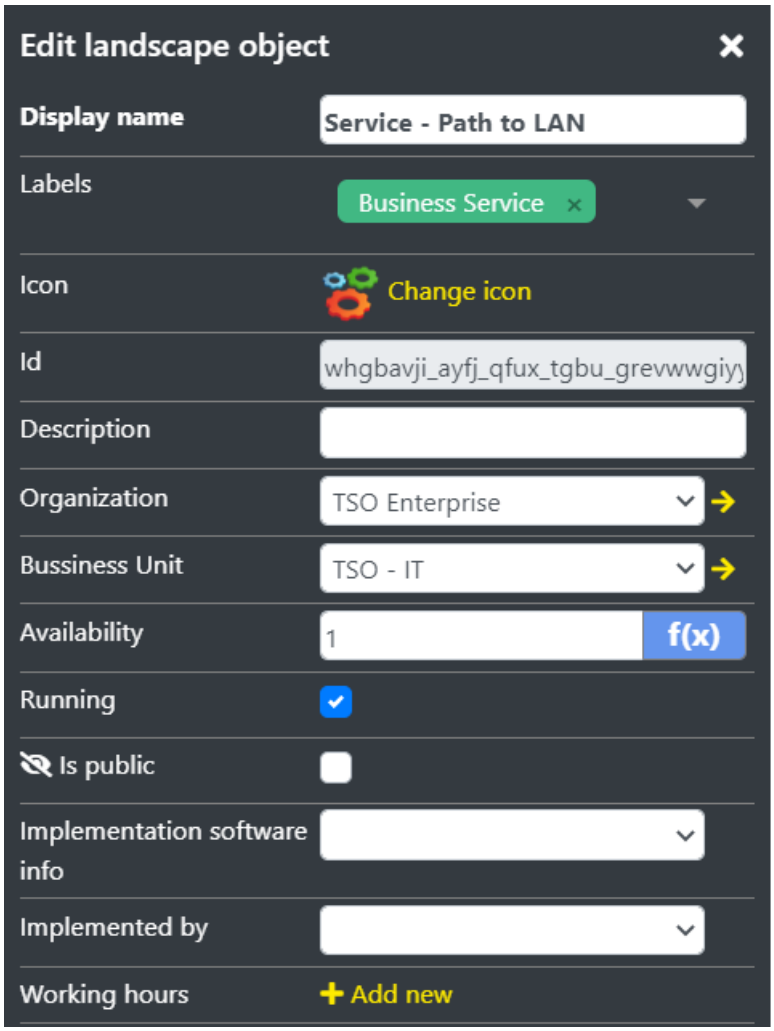
Budući da će se pri simulaciji stvarnog napada trebati provjeravati što se događa sa svim računalima koja su potencijalno kompromitirana za vrijeme napada, trebat će provjeravati je li velik broj računala uključen i spojen na mrežu. Kako bi formule u objektima s oznakom *Record Loss* ostale pregledne i čitljive, takve provjere se mogu napraviti pomoću formula u objektima s oznakom *Business Service*. Najprije je potrebno napraviti takve objekte. Na slici Slika 3.8 stvoren je objekt *Service – Path to LAN*, to je poslovni servis koji će provjeravati dostupnost odabranih računala u mreži. Razinu dostupnosti računala u mreži će određivati formula upisana u atribut *Availability* klikom na gumb *f(x)*. Formula (2) će provjeravati postoji li put između dva odabrana čvora, u ovom slučaju računala i lokalne mreže u kojoj se nalazi, te ako je računalo povezano s mrežom vrijednost atributa *Availability* će biti 1, a inače 0.

$$\text{PathExists (SKAPC01, LAN SKA, time)} \quad (2)$$

Sada je potrebno modificirati formulu (1) u formulu (3) tako da se dio formule (1) koji se sada računa u objektu *Service – Path to LAN* zamijeni s vrijednosti atributa *Availability* tog objekta. Budući da se šteta ne smije generirati kada je računalo spojeno na mrežu i vrijednost atributa *Availability* iznosi 1, šteta se generira ovisno o tome koliko se atribut *Availability* razlikuje od jedinice.

Accumulator (Loss IT. Loss, (1 – Service – Path to LAN. Availability) * 1.3888889, time) (3)

Kako bi izračunata šteta bila vidljiva pri preuzimanju dnevnika zapisa cijele simulacije, potrebno je napraviti *Indicator* element. Na slici Slika 3.9 dani je primjer *Indicator* elementa koji služi za prikaz štete u *Loss IT* objektu. Formula koju je ovdje potrebno upisati je formula koja zaokružuje vrijednost izračunatog gubitka na cijeli broj.

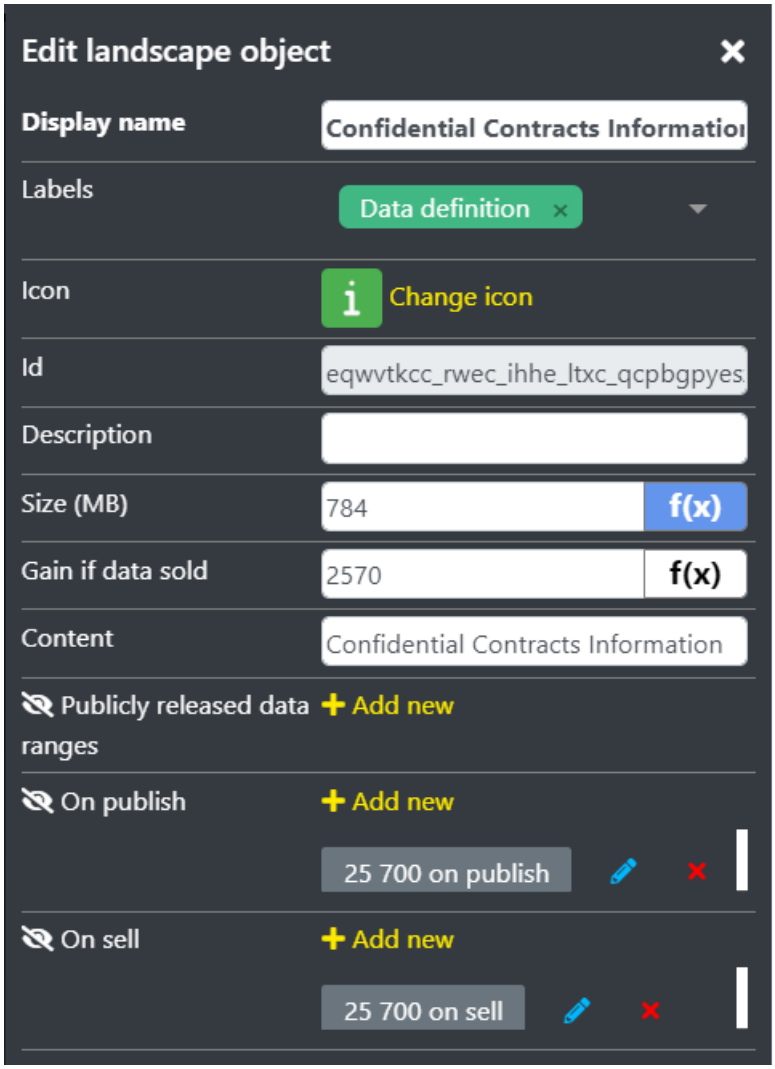


Slika 3.8 Stvaranje objekta s oznakom Business Service

U simulatoru je moguće i definirati kolika će šteta nastati ako se povjerljivi podaci objave ili prodaju od strane napadača. To se radi podešavanjem atributa *On sell* i *On publish* objekata s oznakom *Data definition* koji predstavljaju definiciju podataka organizacije. Primjer jednog takvog objekta dan je na slici Slika 3.10. Moguće je odrediti veličinu podatka, definirati kolika je zarada napadaču kada taj podatak ukrade te o kakvim se podacima radi. Nakon što se objavi ili proda dokument s ovako definiranim podacima, vrijednost atributa *Publicly released data ranges* se postavlja na raspon u kojem su podaci

objavljeni. Time se osigurava da se šteta ne izračunava višestruko ako su objavljeni ili prodani dokumenti koji sadrže iste podatke. Šteta se izračunava tako da se pomnoži broj objavljenih ili prodanih podatka s vrijednosti atributa *On sell* ili *On publish* ovisno o akciji koja je poduzeta nad podacima.

Slika 3.9 Indicator element za prikaz štete



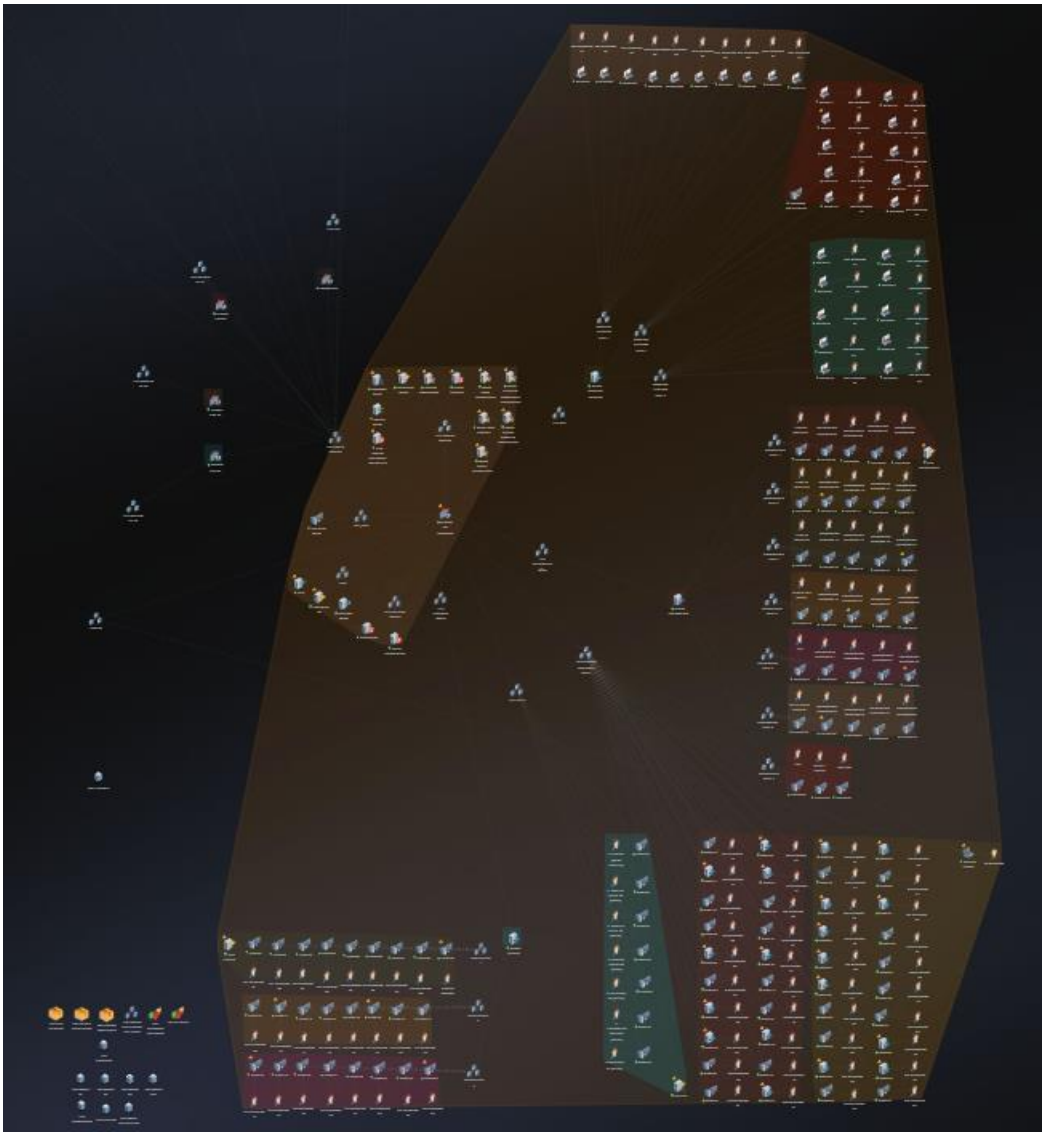
Slika 3.10 Objekt za definiranje podatka

4. Demonstracija izračuna štete za generičku organizaciju

Organizacija na kojoj će se raditi demonstracija izračuna štete je napravljena prema modelu organizacije Hrvatski operator prijenosnog sustava d. d. (HOPS d. d.) [19]. Radi se o operatoru prijenosnog sustava (engl. *Transmission System Operator* - TSO) koji se brine o dostavi električne energije od elektrana do sustava za raspodjelu električne energije [16]. Topologija organizacije *TSO Enterprise* u simulatoru je pojednostavljena u odnosu na stvarnu topologiju HOPS-a i podijeljena je u dva dijela, *information technology (IT) network* (Slika 4.1) i *operational technology (OT) network* (Slika 4.2). IT mreža je podijeljena u pet poslovnih jedinica: *Finance sector (FIN), Business integration sector (BIS), Management department (MAN), Sales Keys Account (SKA) department* i *IT department.* Za svaku od poslovnih jedinica su simulirani zaposlenici i računala koja koriste te lokalne mreže na koje se spajaju. IT mreža je s ostatkom organizacije spojena pomoću objekta *TSO Optical Network.* OT mreža se sastoji od Nacionalnog dispečerskog centra (NDC) u Zagrebu i mrežnih centara upravljanja u Rijeci, Splitu, Osijeku i Zagrebu [20]. Svaki od mrežnih centara nadzire upravljanje dvije od osam trafostanica smještenih na području cijele Hrvatske. Uz *TSO Enterprise*, na topologiji se nalaze i simulirana Tvrtka za brzi odaziv (engl. *RRT Company*), nekoliko partnerskih organizacija (engl. *Trusted partner*) i napadačka organizacija (engl. *Attacker organization*).

Simulacija napada i obrane se sastoje od sekvence napadačkih akcija i sekvence obrambenih akcija. U napadačkoj sekvenci napadač najprije postavlja zloćudni kôd na *mail server* kojem pristupaju zaposlenici *TSO Enterprisea.* Nakon toga radi izviđanje organizacije proučavajući sva računala koja su pristupila zaraženom serveru te za njih stvara *spear phishing mailove*. Uspijeva na dio računala postaviti svoj zloćudni kôd i preko njih pristupiti drugim dijelovima TSO mreže te s tih računala učitati dokumente s povjerljivim podacima organizacije na server pod svojom kontrolom. Budući da su neki zaposlenici primijetili da se radi o potencijalnom *phishingu,* prijavljuju sumnjivu e-poštu svojim nadređenim te u ovom trenutku počinje obrambena sekvenca. Radi se analiza sumnjivog maila te se analizira pristup web mjestu s kojeg je mail došao. Provjeravaju se i ostala računala koja su pristupala sumnjivom web mjestu te je na nekima pronađen

zloćudni program. Organizacija traži pomoć tvrtke za brzi odaziv koja analizira o kakvom se zloćudnom programu radi i na temelju novih informacija se radi daljnja provjera sustava kako bi se otkrila sva zaražena računala. Zaposlenike organizacije se upozorava da pripaze na sumnjive mailove, te se sve otkrivene zloćudne datoteke šalju prodavaču antivirusnog programa kako bi se i one u budućnosti detektirale. Ažuriraju se programska podrška i sustavi za koje se otkrilo da imaju potencijalne ranjivosti. Na samom kraju simulacije napadač prodaje jedan od ukradenih dokumenta s povjerljivim podacima, a drugi objavljuje.

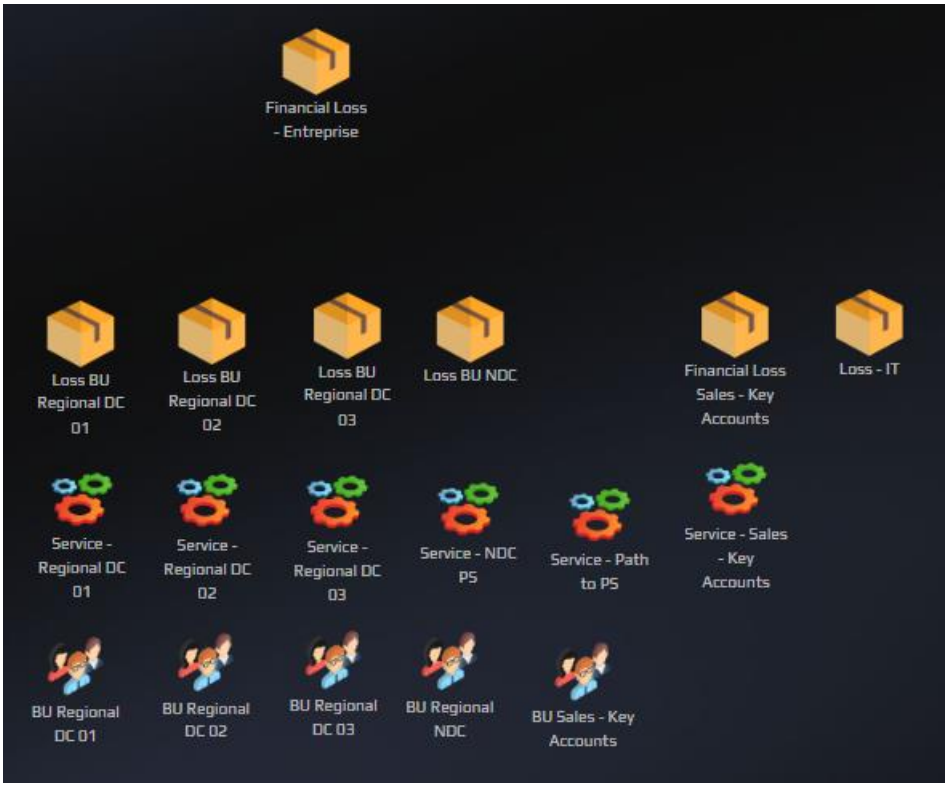


Slika 4.1 IT *network* organizacije *TSO Enterprise*

Slika 4.2 *OT network* organizacije *TSO Enterprise*

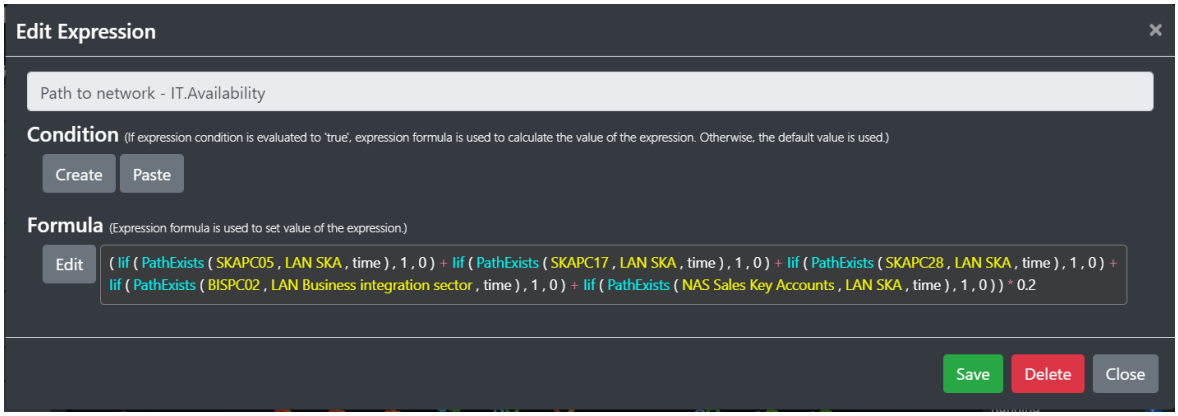
4.1. Šteta koju računa CCS

U topologiji postoje općenito formule koje provjeravaju da nije došlo do isključenja vatrozida ili jedne od trafostanica, no s obzirom na napadačku sekvencu ne očekuje se da će obrana napraviti neku od takvih akcija. Stoga su dodane formule koje provjeravaju što se događa s napadnutim dijelovima sustava u odabranoj napadačkoj sekvenci. Prije dodavanja objekata s dodatnim formulama, dio topologije vezan uz izračun štete prikazan je na slici Slika 4.3.



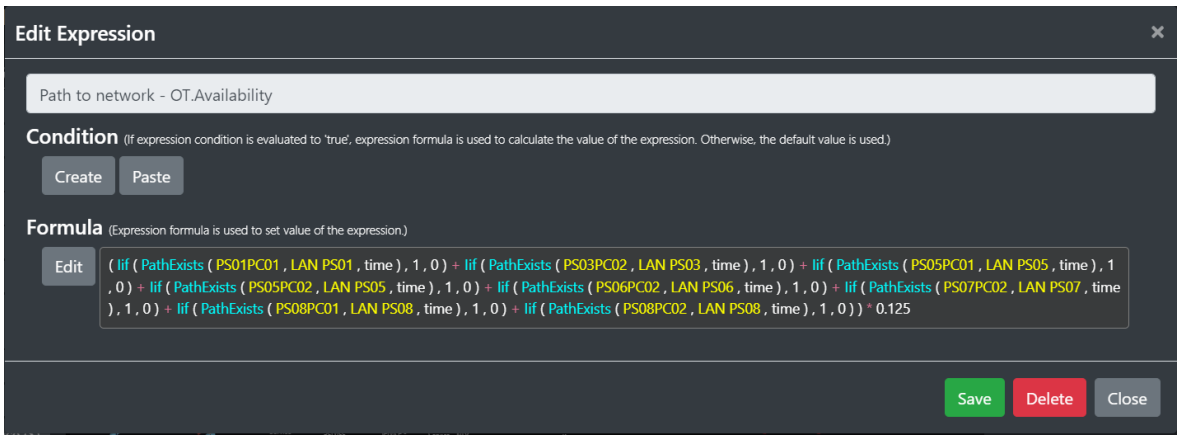
Slika 4.3 Objekti za izračun štete prije dodavanja novih formula

Formule su upisane u simulator prema uputama iz poglavlja 3.1.1. Stvorena su dva objekta s oznakom *Business Service* koja provjeravaju jesu li računala u IT i OT mreži spojena s ostatkom mreže. Objekt koji provjerava jesu li računala u IT mreži spojena s ostatkom mreže je *Path to network – IT* koji je pridružen poslovnoj jedinici *TSO – IT*. Na slici Slika 4.4 je formula pridružena atributu *Availability* tog objekta koja za svako od računala koje bi potencijalno moglo biti odspojeno s mreže tijekom obrambene sekvence provjerava je li ono povezano sa svojom lokalnom mrežom. Vrijednosti su zbrojene i skalirane s faktorom 1 / <broj_računala> kako bi vrijednost atributa *Availability* ostala u intervalu [0, 1].



Slika 4.4 Formula za *Path to network – IT*

Analogno je napravljen objekt *Path to network – OT*. Slika 4.5 prikazuje formulu pridruženu atributu *Availability* tog objekta.



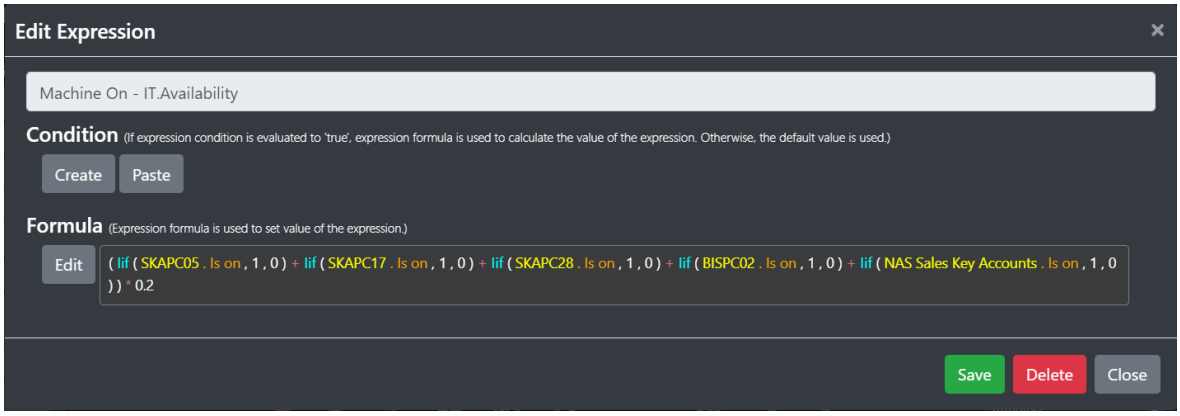
Slika 4.5 Formula za *Path to network – OT*

Šteta povezana s odspajanjem računala s lokalne mreže računati će se u objektu *Loss – IT* u atributu *Loss* gdje na postojeću formulu potrebno dodati formulu (4). Gubitak se povećava što je više računala odspojeno s mreže, odnosno što je vrijednosti atributa *Path to Network.Availability* manja. Procjenjuje se da zaposlenik može obavljati 30 % posla bez da mu je računalo spojeno na Internet [23], stoga se šteta množi s koeficijentom 0.7, a procijenjena šteta po minuti kada računalo nije spojeno na mrežu je 427 $/min, odnosno pretvoreno u sekunde to je 7.1166 $/sek.

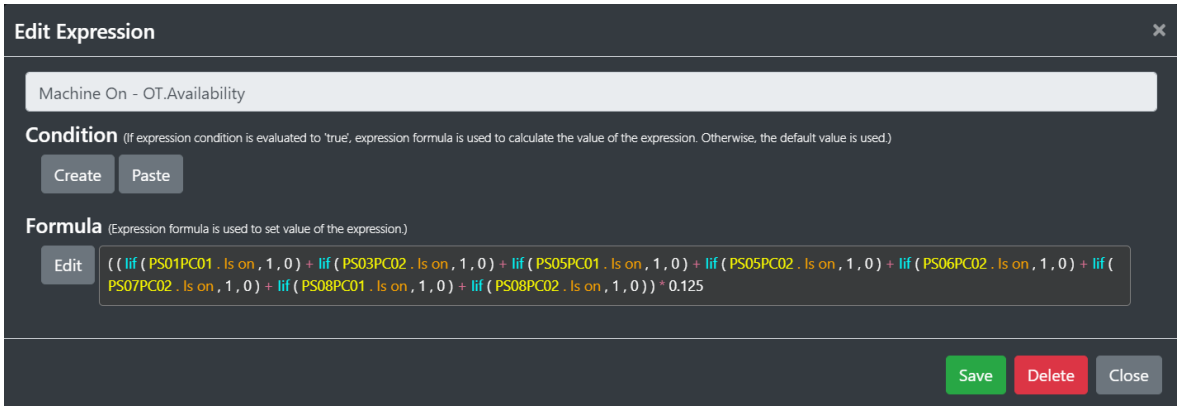
$$\text{Accumulator (Loss - IT. Loss, (1 – Path to Network - IT. Availability) * 0.7 * 7.1166 + (1 – Path to Network - OT. Availability) * 0.7 * 7.1166, time)} \quad (4)$$

Ako računalo nije samo odspojeno s mreže nego je u potpunosti ugašeno, zaposlenik uopće ne može obavljati svoj posao. Takvi gubitci izračunavaju se pomoću formula u objektima *Machine On – IT* i *Machine On – OT* s oznakama *Business service*. Formule prikazane na slikama Slika 4.6 i Slika 4.7 su analogne formulama na slikama Slika 4.4 i Slika 4.5, samo što umjesto provjere postoji li put između dva čvora u mreži ove formule provjeravaju je li atribut *Is on* odabranih računala postavljen na pozitivnu vrijednost.

Šteta povezana s gašenjem računala računati će se u objektu *Loss BU NDC* u atributu *Loss* prema formuli (5), analogno izračunu štete u objektu *Loss – IT* samo što se šteta neće množiti s faktorom 0.7 jer je pretpostavka da ako je računalo ugašeno zaposlenik ne može obavljati svoj posao.



Slika 4.6 Formula za objekt *Machine On – IT*

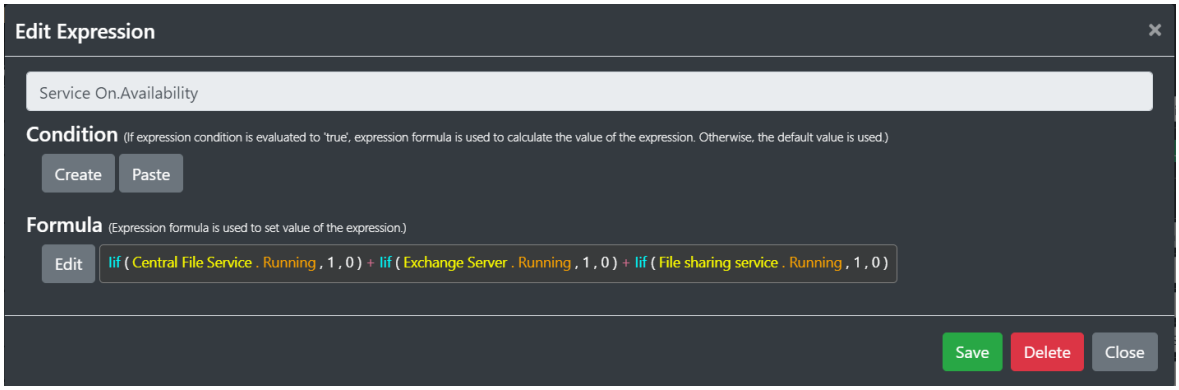


Slika 4.7 Formula za objekt *Machine On – OT*

$$\text{Accumulator (Loss BU NDC. Loss, (1 – Machine On - IT. Availability) * 7.1166 + (1 – Machine On - OT. Availability) * 7.1166, time)} \quad (5)$$

Vrlo slično provjeri je li računalo dostupno, radi se provjera jesu li odabrani servisi dostupni. Ta provjera se radi u objektu *Service On* s oznakom *Business service*, u čiji atribut *Availability* se upisuje formula sa slike Slika 4.8. Razlika je u tome da se za računala provjerava je li atribut *Is on* aktivan, dok se za servise provjerava atribut *Running* te da atribut *Availability* poprima vrijednosti iz intervala [0, 3]. Šteta koju generiraju ugašeni servisi spremat će se u objekt *Financial Loss Sales – Key Accounts* te će se ponovo već upisana formula u tom objektu nadopuniti s formulom (6).

$$\text{Accumulator (Financial Loss Sales - Key Accounts. Loss, (3 – Service On. Availability) * 93.33333, time)} \quad (6)$$



Slika 4.8 Formula za objekt *Service On*

Kada u simulaciji napadač objavi ili proda povjerljive dokumente koje je ukrao od organizacije, na topologiji se pojavljuju objekti *8 600 on publish* i *27 500 on sell* u kojima je izračunata ukupna šteta za organizaciju ovisno o količini podataka koja je objavljena ili prodana kako je opisno u poglavlju 3.1.1. Ukupna šteta za te akcije je pohranjena u atributima *Loss* tih objekata. Štetu koju generiraju formule može se pogledati nakon preuzimanja dnevnika simulacije u listu *Indicators.* U stupcima *Financial Loss – IT ($)* i *Financial Loss - NDC ($)*, šteta se počinje generirati kada se pokrene akcije obrane *Install Security Update for OS* na računala za koja se sumnja da su kompromitirana tijekom napada budući da ta akcija privremeno gasi računalo. Analogno se šteta generira u *Financial Loss - Key Account Losses ($)* kada se pokrene akcija *Install Security Update for Software.*

4.2. Šteta koju računa skripta iz dnevnika simulacije

Nakon što su izvršene sve akcije napada i obrane u simulatoru, preuzet je dnevnik simulacije. Kako bi se izračunala ukupna šteta nakon napada u organizaciji, analizirat će se dnevnik simulacije pomoću Python skripte. Kôd skripte je dostupan na poveznici u dodatku A. U izračunu su korištene procjene svih parametara koji nisu dani u dnevniku simulacije te su te procjene dane u tabličnom obliku u dodatku B.

U listu *Indicators* je prikazana šteta izračunata u simulatoru. Ukupna šteta koju je izračunao simulator dobiva se zbrajanjem šteta u zadnjem retku s podacima u listu *Indicators* i šteta generiranih u objektima *8600 on publish* i *27500 on sell* te će one biti samo pribrojene ostatku štete koju računa skripta.

U listu *Chronology* najprije je potrebno filtrirati samo one zapise čiji je tip *Action* te među njima izdvojiti one koje je provela organizacija koja se brani tijekom napada, odnosno one akcije koje nije napravio igrač *APT Grupa*. Za svaku od obrambenih akcija šteta je računata kao formula (6), gdje je procjena cijene rada zaposlenika uzeta iz učitane datoteke *Models.py* u kojoj se nalaze procjene svih parametara koji nisu dani u dnevniku simulacije.

(vrijeme potrebno da se akcija izvede) * (cijena rada zaposlenika koji obavlja akciju) (6)

Posebno, za neke akcije su izračunati dodatni troškovi koje one generiraju. Izračunata je šteta koja nastaje nadogradnjom sustava. Dio te štete već je pribrojio simulator jer tijekom nadogradnje računala nisu bila raspoloživa. U skripti je izračunati trošak koji nastaje zbog kupovine novih licenci te troškovi edukcija zaposlenika kako koristiti novi sustav. U obzir je uzeti i trošak koji nastaje zbog smanjene produktivnosti zaposlenika kada se privikavaju na novi sustav. Izdvojen je trošak povezan s *RRT Company* kako bi se kasnije moglo razmotriti treba li taj trošak pribrojiti šteti od napada ili bi taj trošak bio pokriven ugovorom koji organizacija ima s *RRT Company*. Posebno je izdvojen i trošak za preseljenje zaposlenika s jedne lokacije na drugu u kojem su uzeti u obzir cijena dnevnica zaposlenicima i troškovi povezani uz vrstu prijevoznog sredstva koji je zaposlenik koristio (cestarine, putni troškovi, cijene karata za prijevozna sredstva). Budući da simulator ne podržava sve akcije koje se u stvarnosti rade vezano uz rješavanje napada, akcije poput pregledavanja politika i pravilnika, unajmljivanja odvjetnika i obavijesti regulatornih tijela da je došlo do napada te plaćanje pravnih troškova, kazni i naknada vezanih uz napad, takvi troškovi su procijenjeni u datoteci *Models.py* i dodatni ukupnoj šteti [8]. Troškovi su podijeljeni u kategorije izravnih i neizravnih troškova, a u svakoj od tih kategorija se nalazi troškovi čiji su izvori objašnjeni u poglavlju 2.1. Uzeti su u obzir samo oni izvori koji imaju smisla u kontekstu simuliranog napada.

Kroz cijeli izračun se mijenja i faktor rizika od daljnjih napada, pa se pri izvršavanju akcije koja detaljno pregledava dio sustava ili ažurira sustav faktor rizika smanjuje, dok se kod akcija koje površno pregledavaju dio sustava ili koje izvršavaju akteri s malim kompetencijama faktor rizika povećava jer postoji mogućnost da se nisu pronašli svi propusti u sustavu.

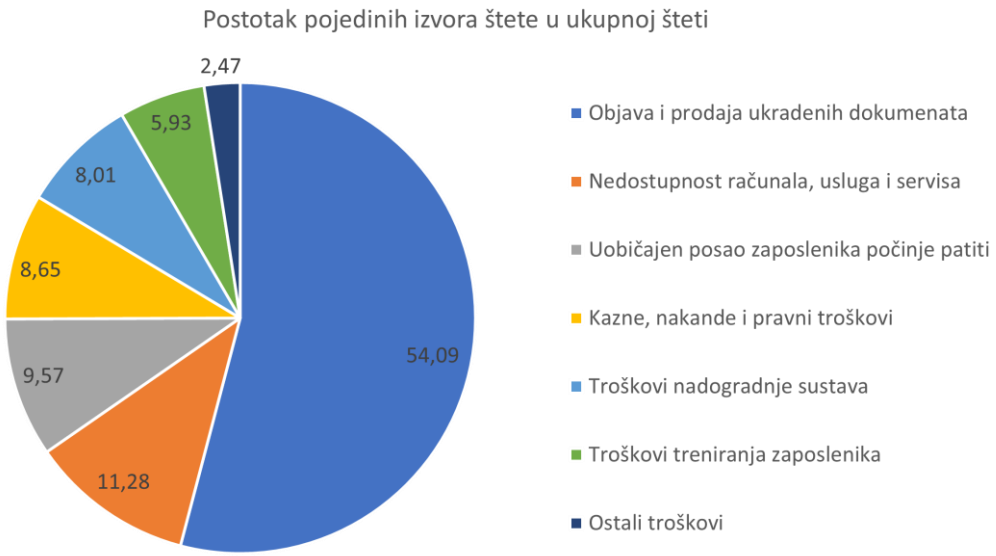
Izračun štete je variran s obzirom na pretpostavke vezane uz organizaciju u šest metoda, sažeti prikaz dobivenih šteta po metodama prikazan je u tablici Tablica 4.1:

1. Prva metoda pretpostavlja da kada zaposlenici obavljaju zadatke vezane uz rješavanje napada njihov uobičajen posao ne pati. Pri treniranju osoblja kako se ponašati kada se otkrije incident unajmljeni su stručnjaci za treniranje te potreban materijal i prostor. Organizacije mora povećati vrijeme otplate kredita zbog povećanog rizika od daljnjih napada i ona nije osigurana od kibernetičkih napada. Ima ugovor s *RRT Company* pa je njihove usluge za vrijeme napada ne koštaju dodatno. Ukupna šteta od napada je 3,018,814.41 $.
2. S obzirom na prvu metodu, jedina razlika u drugoj metodi je ta da normalan posao zaposlenika počinje patiti nakon jednog radnog dana pa on počinje generirati štetu. Budući da su zaposlenici plaćeni i rade unutar normalnog radnog vremena bez obzira na vrstu posla koji obavljaju, ovdje se ne uračunava trošak izračunat prema formuli (6). Ukupna šteta od napada je 3,356,504.96 $.
3. U odnosu na drugu metodu, mijenja se način treniranja zaposlenika kako reagirati kada dođe do incidenta u organizaciji. Umjesto unajmljivanja stručnjaka za provedbu treninga te iznajmljivanja prostora i materijala potrebnih za vježbu, zaposlenicima je plaćen online tečaj za treniranje. Ukupna šteta od napada je 3,561,202.88 $.
4. Četvrta metoda u odnosu na treću pretpostavlja da organizacija trenutno ne otplaćuje kredit te da je osigurana od kibernetičkog napada i osiguranje joj je isplatilo policu u visini 1,000,000.00 $. Ukupna šteta od napada umanjena za iznos police osiguranja je 2,564,626.23 $.
5. U petoj metodi se trošak iz treće metode uvećava za izračunati faktor rizika zbog nepredviđenih budućih troškova i veće mogućnosti od daljnjih napada. Ukupna šteta od napada u ovom slučaju iznosi 3,567,264.07 $.
6. Šesta metoda izračunava maksimalnu štetu s obzirom na predviđene izvore štete i pretpostavlja da normalan posao počinje patiti nakon jednog radnog dana, da je organizacija platila online tečaj za treniranje svojih zaposlenika te da nema ugovor s *RRT Company* i mora unajmiti njezine usluge kada dođe do incidenta. Također, otplaćuje kredit u banci i mora produljiti vrijeme otplate te nije osigurana protiv kibernetičkog napada. Uz to, štetu uvećava za faktor rizika zbog nepredviđenih troškova koje bi mogla imati vezano uz napad. Ukupna šteta u ovom slučaju je 3,567,882.60 $.

Tablica 4.1 Ukupna šteta nakon napada ovisno o metodi izračuna

Metoda	Ukupna ekonomska šteta nakon kibernetičkog napada
Metoda 1	3,018,814.41 $
Metoda 2	3,356,504.96 $
Metoda 3	3,561,202.88 $
Metoda 4	2,564,626.23 $
Metoda 5	3,567,264.07 $
Metoda 6	3,567,882.60 $

S obzirom na metode izračuna, ukupna šteta najviše varira ovisno o tome pati li uobičajen posao zaposlenika za vrijeme rješavanja napada ili ne. Ukupna šteta se značajno smanjuje kada je organizacija osigurana od kibernetičkog napada. Promatrajući sve izvore štete koji su uzeti u obzir pri izračunu i ukupnu štetu koja je dobivena s pretpostavkama iz šeste metode mogu se odrediti izvori koji najviše doprinose ukupnoj ekonomskoj šteti nakon napada (). Trošak od objave ili prodaje ukradenih dokumenata s povjerljivim podacima predstavlja 54.09% ukupne štete. Nedostupnost računala, usluga i servisa generira 11.28% ukupne štete. Trošak koji se stvara kada uobičajen posao zaposlenika počinje patiti predstavlja 9.57% dok kazne, naknade i pravni troškovi generiraju 8.65% ukupne štete. Troškovi nadogradnje sustava čine 8.01%, a troškovi treniranja zaposlenika uz pomoć online tečaja čine 5.93%. Svi ostali izvori štete spadaju u preostalih 2.47% ukupne štete.



Slika 4.9 Grafički prikaz koliko pojedini izvor štete pridonosi ukupnoj šteti

4.3. Usporedba s literaturom

Prema [21] prosječna šteta od kibernetičkog napada u energetskoj industriji iznosi 4,650,000.00 $ što je nešto više od prosječne štete od kibernetičkog napada u svijetu u prošloj godini koja iznosi 4,350,000.00 $ [22]. S druge strane [7] i [8] procjenjuju štetu od kibernetičkog napada na iznose koji se kreću oko milijun dolara. Ekonomske štete variraju ovisno o veličini organizacije, uvjetima u kojima se napad dogodio i industrijskom sektoru u kojem organizacija posluje stoga se može zaključiti da je ukupna šteta izračunata na temelju podataka iz simulatora i nekih pretpostavki dobra procjena ukupne ekonomske štete.

Glavni troškovi od kibernetičkog napada su troškovi nastali pri inicijalnom rješavanju napada i troškovi nadogradnje sustava kako bi se daljnji napadi spriječili, troškovi vezani uz nedostupnost podataka, servisa i usluga, troškovi od plaćanja kazni i naknada te troškovi povezani uz gubitak intelektualnog vlasništva. Najzastupljeniji izvori štete pri izračunu ukupne štete od simuliranog napada uglavnom spadaju u ove kategorije.

5. Zaključak

Ekonomska šteta izračunata pomoću CCS-a i Python skripte nalazi se u očekivanom intervalu štete za veličinu i vrstu organizacije koja je simulirana te vrsti napada koji je proveden. Može se smatrati dobrom procjenom kolika bi ekonomska šteta bila da se napad zapravo dogodio. Simulator kibernetičkih napada može, uz obučavanje sudionika kako se nositi s napadom, podizati svijest kolika ekonomska šteta nastaje kada dođe do napada. Time se organizacije mogu pravovremeno pripremiti na takve izdatke i razmotriti osiguranja od kibernetičkog napada za koja je pokazano u demonstraciji da značajno smanjuju ukupnu štetu.

Budući da simulator ima neka ograničenja, trebalo bi ga nadograditi s dodatnim akcijama kojima bi se mogli simulirati ostali izvori šteti koji su pretpostavljeni pri izračunu sa skriptom. Neke od akcija koje bi se mogle dodati su testiranje sustava, treniranje zaposlenika, provjera je li došlo do krađe financijskih sredstava, mogućnost ručnog upravljanja strojevima, popravak ili zamjena oštećenih strojeva, obavještavanje regulatornih tijela da je došlo do incidenta te obavještavanje klijenata da su njihovi podaci kompromitirani tijekom napada. Akcija *Request Assistance* bi se mogla nadopuniti s opcijama da se pomoć može potražiti i od odvjetnika, tvrtki koje se bave odnosima s javnošću te privremenim zapošljavanjem novih zaposlenika. Općenito bi se u topologiju trebale dodati banke, osiguranja, odvjetnički uredi i tvrtke za odnose s javnošću. Također, mogla bi se simulirati promjena cijene dionica te promjena broja klijenata kroz vrijeme kako bi se olakšao izračun neizravnih izvora štete. Kao što se trenutno generiraju objekti *on sell* i *on publish,* trebali bi se generirati i objekti s kaznama, naknadama i troškovima pravnih sporova. Svaka akcija utječe na promjenu faktora rizika od budućih napada pa bi se i on mogao ugraditi u simulaciju. Kod samih formula za izračun štete bi se trebale dodati funkcije i operacije pomoću kojih bi se mogle pisati matematički kompleksnije formule kako bi što bolje predviđala šteta. Upisivanje formula bi bilo brže i jednostavnije da se formule mogu upisivati kao tekst. Također, trebala bi postojati i opcija odabira valute u kojoj se šteta računa te bi se ta valuta automatski trebala ubaciti u naziv stupaca u dnevniku simulacije koji su vezani uz izračun štete. Time bi se dio izračuna koji se radi sa

skriptom smanjio i način izračuna bi se generalizirao budući da je trenutni izračun u skripti vezan uz topologiju organizacije u simulatoru.

Popis izvora štete s početka rada i opis postupka upisivanja formula u simulator trebao bi pomoći svim sudionicima kibernetičkih vježbi lakše i brže predvidjeti ekonomsku štetu nakon kibernetičkog napada.

6. Literatura

[1] HNB, “Kreditna sposobnost,” 2. lipnja 2020. [Online]. Dostupno: Kreditna sposobnost - HNB [Pristupljeno 13. svibnja 2023.]

[2] A. M. Algarni and Y. K. Malaiya, "A consolidated approach for estimation of data security breach costs," *2016 2nd International Conference on Information Management (ICIM)*, London, UK, 2016, pp. 26-39.

[3] H. Heyburn, A. Whitehead, L. Zanobetti, J. N. Shah and S. Furnell, “Analysis of the full costs of cyber security breaches,” Ipsos MORI, Final report, 2020.

[4] Laboratorij za informacijsku sigurnost i privatnost, “Projekti: Cyber Conflict Simulator,” *Fakultet elektrotehnike i računarstva*, [Online]. Dostupno: Projekti - Laboratorij za informacijsku sigurnost i privatnost (unizg.hr) [Pristupljeno 13. Svibnja 2023.]

[5] Predavanje iz Sigurnosti računalnih sustava, Tema: “Osnovni pojmovi i uvod u sigurnost.” Računarstvo, Fakultet elektrotehnike i računarstva, Zagreb, 2023.

[6] IBM Newsroom, “IBM Report: Cost of a Data Breach Hits Record High During Pandemic,” 28. srpnja 2021. [Online]. Dostupno: IBM Report: Cost of a Data Breach Hits Record High During Pandemic [Pristupljeno 13. svibnja 2023.]

[7] T. Caldwell, “The true cost of being hacked.” *Computer Fraud & Security*, vol. 2014., issue 6, pp. 8-13, 2014.

[8] R. Layton and P. A. Watters, “A methodology for estimating the tangible cost of data breaches,” *Journal of Information Security and Applications*, vol. 19, issue 6, 2014, pp. 321-330

[9] V. McGrath, E. Sheedy and F. Yu, “Governance of cyber security: State of play,” Cyber Security Hub, Optus Macquarie University, siječanj 2022.

[10] M. Riek, R. Boehme, M. Ciere, C. Hernandez Ganan and M. van Eeten, “Estimating the costs of consumer-facing cybercrime: A tailored instrument and representative data for six EU countries,” In Proceedings of Workshop of Economics of Information Security, 2016, pp. 1-43

[11] S. Patel and J. Zaveri, “A Risk-Assessment Model for Cyber Attacks on Information Systems,” *Journal of Computers*, no. 5, pp. 352-359, 2010.

[12] J. Haislip, K. Kolev, R. Pinsker and T. Steffen, “The economic cost of cybersecurity breaches: A broad-based analysis,” Workshop on the Economics of Information Security (WEIS), 9. svibnja 2019.

[13] I. Tomašević, “Sustavi nadzora i upravljanja (SCADA) u energetici,” Završni rad, Fakultet elektrotehnike, računarstva i informacijskih tehnologija, Osijek, 2019.

[14] P. Dreyer, T. Jones, K. Klima, “Estimating the Global Cost of Cyber Risk,” RAND Corporation, Santa Monica, California, 2018.

[15] Span Cyber Security Center, “Cyber Security Training Catalogue,” *Span*, [Online]. Dostupno: https://www.span.eu/media/1kuhagxg/cyber-security-training-catalogue.pdf [Pristupljeno: 18. svibnja 2023.]

[16] Utilis d. o. o. osoblje, *Roles and Communication during Serious Cyber Incident in an Operator of Critical Services*, Utilis d. o. o, 2022.

[17] K. Grubešić, “Izgradnja složenog kibernetičkog poligona za vježbe napada i obrane,” Diplomski rad, Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu, srpanj 2022.

[18] Cyber Conflict Simulator Utilis d. o. o., “Cyber Conflict Simulator – Kako radi?,” *Utilis d. o. o.*, 2021. [Online]. Dostupno: Kako radi? (utilis.biz) [Pristupljeno: 18. svibnja 2023.]

[19] HOPS d. d., “O nama, ” *HOPS d. d.*, 2023. [Online]. Dostupno: https://www.hops.hr/o-nama [Pristupljeno: 21. svibnja 2023.]

[20] HOPS d. d., “Model vođenja EES-a,” *HOPS d. d.*, 2023. [Online]. Dostupno: https://www.hops.hr/model-vodenja-ees-a [Pristupljeno: 21. svibnja 2023.]

[21] Dawn Allcot, “Report: Cost of a Data Breach in Energy and Utilities,” *Security Intelligence*, 2021. [Online]. Dostupno: Report: Cost of a Data Breach in Energy and Utilities (securityintelligence.com) [Pristupljeno: 21. svibnja 2023.]

[22] IBM Security, “Cost of a Data Breach Report 2022: Executive Summary,” IBM Security, 2022.

[23] Deloitte, “The economic impact of disruptions to Internet connectivity. A report for Facebook,” Deloitte, listopad 2016.

Sažetak

Određivanje ekonomske štete u organizaciji nastale kao posljedica kibernetičkog napada

Određivanje ekonomske štete u organizaciji predstavlja izazov jer organizacije često nisu svjesne koji sve izvori štete postoje pa je na početku rada dan pregled svih izvora štete nakon kibernetičkog napada. Oni su podijeljeni na izravne i neizravne izvore štete te detaljno opisani. Nakon toga je predstavljen *Cyber Conflict Simulator* u kontekstu definiranja formula za izračun ekonomske štetu unutar simulatora. Pomoću simulatora je napravljena simulacija napada i obrane na operator prijenosnog sustava te je pomoću formula definiranih u simulatoru i Python skripte izračunata ekonomska šteta za taj napad. Varirani su izvori štete te se pratila promjena ukupno iznosa ekonomske štete te su se odredili izvori štete koji joj najviše pridonose.

Ključne riječi: ekonomska šteta, kibernetički napad, *Cyber Conflict Simulator*, formule za izračun štete, izvori ekonomske štete, troškovi, operator prijenosnog sustava

Summary

Determining the economic damage in an organization as a result of a cyber attack

Determining the economic damage in an organization is a challenge because organizations are unaware of what sources of economic damage exist, so at the start of the thesis, there is a review of all damage sources after a cyber attack. They are divided into direct and indirect costs and described in detail. After that, the Cyber Conflict Simulator is presented in the context of defining formulas for calculating economic damage within the simulator. Simulation of an attack and defense on the transmission system operator is made, and the cost of that attack is calculated using equations in the simulator and Python script. The sources of damage are varied, the total amount of damage is monitored, and the origin of damage that contributed the most to it is determined.

Keywords: economic damage, cyber attack, Cyber Conflict Simulator, equations for calculating damage, sources of economic damage, cost, transmission system operator

Skraćenice

CCS	*Cyber Conflict Simulator*	simulator kibernetičkih napada
TSO	*Transmission System Operator*	operator prijenosnog sustava
SCADA	*Supervisory Control and Data Acquisition*	sustav nadzora i upravljanja
IT	*information technology*	informacijska tehnologija
OT	*operational technology*	upravljačka tehnologija
FIN	*finance sector*	financijski sektor
BIS	*business integration sector*	sektor poslovne integracije
MAN	*management department*	rukovodstvo
SKA	*sales key accounts*	

Dodatak A: Programski kod

Programski kôd za izračun štete na temelju dnevnika zapisa preuzetog iz simulatora dostupan je na poveznici: https://gitlab.com/ccs-loss/zavrsni-rad

Dodatak B: Tablica s procjenama šteta

Tablica s procjenama šteta za pojedini dio izračuna u poglavlju 4.

Varijabla	Cijena	Poveznica	Datum
IT Log Admin 05 (junior)	21.5 $/h	https://www.payscale.com/research/US/Job=Junior_Systems_Administrator/Hourly_Rate/0b1b54aa/Portland-OR	7.5.2023
IT Director (senior Sys&Log)	95.0 $/h	https://www.salary.com/research/salary/benchmark/information-technology-director-hourly-wages	7.5.2023
CEO	393.0 $/h	https://www.salary.com/research/salary/benchmark/chief-executive-officer-hourly-wages	7.5.2023
RRT Forensics 01	48.0 $/h	https://www.salary.com/tools/salary-calculator/computer-forensics-analyst-i-hourly	7.5.2023
OT DC 03 Sys&Log Admin 01 (senior)	58.0 $/h	https://www.salary.com/tools/salary-calculator/system-administrator-senior-unix-hourly	7.5.2023
IT Sys&Log Admin 02 (senior)	58.0 $/h	https://www.salary.com/tools/salary-calculator/system-administrator-senior-unix-hourly	7.5.2023
IT Sys&Log Admin 04 (junior)	29.92 $/h	https://www.zippia.com/junior-systems-administrator-jobs/salary/	7.5.2023
IT Sys&Log Admin 03 (senior)	58.0 $/h	https://www.salary.com/tools/salary-calculator/system-administrator-senior-unix-hourly	7.5.2023
RRT Reversing 01	65.0 $/h	https://www.salary.com/research/salary/posting/malware-reverse-engineer-hourly-wages	7.5.2023
PS07 IT technican 01	25.0 $/h	https://www.salary.com/tools/salary-calculator/information-system-technician-hourly	7.5.2023
IT Log&Backup Admin 01 (senior)	47.0 $/h	https://www.salary.com/tools/salary-calculator/storage-backup-recovery-specialist-ii-hourly	7.5.2023
OT DC 01 Sys&Log Admin 01 (senior)	58.0 $/h	https://www.salary.com/tools/salary-calculator/system-administrator-senior-unix-hourly	7.5.2023
TSO CISO	113.0 $/h	https://www.salary.com/tools/salary-calculator/ciso-hourly	7.5.2023
OT DC 01 Sys&Log Admin 02 (senior)	58.0 $/h	https://www.salary.com/tools/salary-calculator/system-administrator-senior-unix-hourly	7.5.2023
OT Director (senior Log&Sys)	92.0 $/h	https://www.salary.com/research/salary/benchmark/engineering-director-hourly-wages	7.5.2023
OT DC 02 Sys&Log Admin 01 (senior)	58.0 $/h	https://www.salary.com/tools/salary-calculator/system-administrator-senior-unix-	7.5.2023

		hourly	
Risk Officer	27.83 $/h	Layton, Robert, and Paul A. Watters. "A methodology for estimating the tangible cost of data breaches." Journal of Information Security and Applications 19.6 (2014): 321- 330.	7.5.2023
Risk Manager	75.91 $/h	Layton, Robert, and Paul A. Watters. "A methodology for estimating the tangible cost of data breaches." Journal of Information Security and Applications 19.6 (2014): 321- 330.	7.5.2023
Customer Service Manager	32.9 $/h	Layton, Robert, and Paul A. Watters. "A methodology for estimating the tangible cost of data breaches." Journal of Information Security and Applications 19.6 (2014): 321- 330.	7.5.2023
Executive Assistant	35.43 $/h	Layton, Robert, and Paul A. Watters. "A methodology for estimating the tangible cost of data breaches." Journal of Information Security and Applications 19.6 (2014): 321- 330.	7.5.2023
Lawyer	200.0 $/h	Layton, Robert, and Paul A. Watters. "A methodology for estimating the tangible cost of data breaches." Journal of Information Security and Applications 19.6 (2014): 321- 330.	7.5.2023
Head of Media Relations	32.9 $/h	Layton, Robert, and Paul A. Watters. "A methodology for estimating the tangible cost of data breaches." Journal of Information Security and Applications 19.6 (2014): 321- 330.	7.5.2023
Policy Officer	27.83 $/h	Layton, Robert, and Paul A. Watters. "A methodology for estimating the tangible cost of data breaches." Journal of Information Security and Applications 19.6 (2014): 321- 330.	7.5.2023
Compliance Officer	27.83 $/h	Layton, Robert, and Paul A. Watters. "A methodology for estimating the tangible cost of data breaches." Journal of Information Security and Applications 19.6 (2014): 321- 330.	7.5.2023
IT Training Officer	50.6 $/h	Layton, Robert, and Paul A. Watters. "A methodology for estimating the tangible cost of data breaches." Journal of Information Security and Applications 19.6 (2014): 321- 330.	7.5.2023
IT Training Manager	63.26 $/h	Layton, Robert, and Paul A. Watters. "A methodology for estimating the tangible cost of data breaches." Journal of Information Security and Applications 19.6 (2014): 321- 330.	7.5.2023
Administration Assistant	18.03 $/h	Layton, Robert, and Paul A. Watters. "A methodology for estimating the tangible cost of data breaches." Journal of Information Security and Applications 19.6 (2014): 321- 330.	7.5.2023
Project Manager	75.9 $/h	Layton, Robert, and Paul A. Watters. "A methodology for estimating the tangible cost of data breaches." Journal of Information Security and Applications 19.6 (2014): 321- 330.	7.5.2023
Executive Manager	75.9 $/h	Layton, Robert, and Paul A. Watters. "A methodology for estimating the tangible cost of data breaches." Journal of Information Security and Applications 19.6 (2014): 321- 330.	7.5.2023

materials	1000 $	https://solo.co/blog/how-much-does-it-cost-to-rent-space-for-a-small-business/	7.5.2023
costOfATrainingCourse	1678 $/zaposlenik	https://www.bizlibrary.com/blog/training-programs/cost-of-training-employees/	7.5.2023
finesForStolenDocument	100000 $/dokument	https://cyberinsureone.com/laws-penalties/	7.5.2023
lawyerCost	8600 $	https://dldlawyers.com/cyber-liability-legal-costs-law-firm/	7.5.2023
settelments	100000 $	https://magoo.medium.com/how-to-estimate-legal-costs-from-a-data-breach-1b523c8b0d72	7.5.2023
totalCreditBefore	46153.59 $	https://www.pbz.hr/gradjani/nenamjenski-krediti/nenamjenski-kredit.html	7.5.2023
totalCreditAfter	52760.88 $	https://www.pbz.hr/gradjani/nenamjenski-krediti/nenamjenski-kredit.html	7.5.2023
insurancePolicyCost	1500 $	https://www.embroker.com/blog/cyber-insurance-cost/	7.5.2023
insuranceCoverage	1000000 $	https://www.embroker.com/blog/cyber-insurance-cost/	7.5.2023
deductible	10000 $	https://www.embroker.com/blog/cyber-insurance-cost/	7.5.2023
travelDailyWage	26.55 $/dan	https://aestus.hr/kako-obracunati-dnevnice-i-putne-troskove/	7.5.2023
pricePerKmWalk	0.4 $/km	https://aestus.hr/kako-obracunati-dnevnice-i-putne-troskove/	7.5.2023
pricePerKmCar	0.68 $/km	https://www.driversnote.ca/blog/travel-expenses-for-employees	7.5.2023
cestarina	30 $	https://www.zagreb-airport.hr/putnici/do-od-zracne-luke/taxi-rent-a-car/177	7.5.2023
taxiToAirport	30 $	https://www.zagreb-airport.hr/putnici/do-od-zracne-luke/taxi-rent-a-car/177	7.5.2023
pricePerKmPlane	0.1 $/km	https://financhill.com/blog/investing/how-much-does-it-cost-to-operate-a-helicopter#:~:text=The%20average%20cost%20for%20an,larger%20flights%20with%20more%20passengers.	7.5.2023
baggageCost	13 $	https://www.croatiaairlines.com/hr/nase-dodatne-usluge/dodatna-prtljaga	7.5.2023
diffLicenceCost	100 $	https://www.forscope.hr/ms-windows-server-2019/?gclid=EAIaIQobChMIiuix-ujR_gIVVrDVCh1yyQL_EAAYASAAEgKnqvD_BwE	7.5.2023
testSW	150 $	Layton, Robert, and Paul A. Watters. "A methodology for estimating the tangible cost of data breaches." Journal of Information Security and Applications 19.6 (2014): 321- 330.	7.5.2023

business downtime	427 $/h	https://www.pingdom.com/outages/average-cost-of-downtime-per-industry/#:~:text=Relatively%20small%20businesses'%20cost%20of,for%20just%20a%20short%20outage	7.5.2023