Sadržaj

1. Uvod

Kontinuiranim razvojem tehnologije, sve veći broj organizacija ovisi o digitalnoj infrastrukturi. Kibernetički napadi postaju sve češći i složeniji te imaju velik utjecaj na svakodnevni život pojedinaca i poslovne procese poduzeća jer im mogu nanijeti znatnu ekonomsku štetu. Posljedice uspješnih kibernetičkih napada mogu biti ozbiljne i najčešće nisu vezane samo za financijske gubitke već i za razne druge dugoročne posljedice kojih žrtve napada nisu odmah svjesne. Stoga je iznimno važno razumjeti načine određivanja ekonomske štete koja može proizaći iz takvih sigurnosnih incidenata, posebno u kontekstu različitih načina obrane koje organizacija primjenjuje. Ekonomska šteta može se definirati kao zbroj različitih vrsta troškova. Poznavanje svih kategorija troškova koji mogu nastati kao posljedica napada omogućava organizacijama bolju procjenu ukupnog troška, odnosno štete. Svrha rada je istražiti kako načini obrane organizacije mogu utjecati na smanjenje ili povećanje ekonomske štete. Ovakav uvid u troškove pružit će organizacijama smjernice za bolje razumijevanje, procjenu i upravljanje ekonomskom štetom te omogućiti donošenje odluka u vezi s ulaganjima u sigurnosne mjere i obrambene strategije.

Rad se sastoji od teorijskog i praktičnog dijela. U teorijskom dijelu opisan je način računanja ekonomske štete i kategorizacija troškova koji se uzimaju u obzir korištenjem znanstvenih i stručnih publikacija dostupnih na internetu. Za potrebe simulacije napada i obrane te računanje određenih vrsta troškova koristi se posebno dizajniran simulator *Cyber Conflict Simulator* (CCS), projekt FER – ovog Zavoda za elektroniku, mikroelektroniku, računalne i inteligentne sustave (ZEMRIS) i tvrtke Utilis d.o.o [1]. Korištenjem CCS-a se na intuitivan i jednostavan način analiziraju taktike i tehnike koje koriste napadači, kao i strategije i tehnologije koje koriste branitelji.

U drugom poglavlju obrađuje se klasifikacija troškova s ciljem identifikacije različitih vrsta troškova koji mogu proizaći iz incidenta, kao i onih koji predstavljaju izazove pri svojoj procjeni. Treće poglavlje je posvećeno CCS-u koji se koristi za izračunavanje

određenih vrsta troškova. U tom poglavlju će biti i detaljno opisana struktura mreže organizacije koja će biti korištena za procjenu nastale štete. U četvrtom poglavlju nalazi se detaljan uvid u korištene formule za izračunavanje štete kao i konkretne brojke koje se koriste za izračun od kojih su neke satnica IT stručnjaka, novčane kazne zbog incidenta i slično. Opisan je napad za koji se variraju tri načina obrane, a potom se za svaki od tih scenarija računa šteta. U petom poglavlju, zaključku, izneseni su rezultati rada. Svi korišteni izvori mogu se pronaći u šestom poglavlju literature koje obuhvaća sve relevantne izvore informacija korištene tijekom izrade ovog rada.

2. Klasifikacija troškova

Kako bi se dobila cjelovita procjena ekonomske štete, potrebno je detaljno razmotriti i raščlaniti različite vrste troškova koji se javljaju. U tu svrhu, analiza koja slijedi omogućuje bolje razumijevanje ukupne štete te pruža osnovu za daljnje ekonomske procjene. Pri računanju troškova, važno je uspostaviti odgovarajuću strukturu koja obuhvaća sljedeće aspekte: kategorizaciju troškova i učinkovito mjerenje troškova. Dakle, potrebno je identificirati i klasificirati troškove prema odgovarajućim kategorijama što omogućuje jasniju analizu i praćenje troškova. Troškovi mogu biti kategorizirani u izravne, neizravne, kratkoročne i dugoročne troškove [4], [12]. Za prikupljanje što preciznijih podataka za računanje troškova, važno je koristiti odgovarajuće metode i alate. Kroz sljedeća potpoglavlja bit će opisani specifični troškovi koji su pripisani određenoj kategoriji. Ovakva podjela na kategorije omogućava bolje strukturiranje i organizaciju informacija, a samim time dobiva se i cjelovit uvid u financijsku situaciju i raspodjelu troškova unutar organizacije.

2.1. Kratkoročni izravni troškovi

Kratkoročni izravni troškovi obuhvaćaju sva financijska plaćanja koja su izvršena tijekom procesa rješavanja incidenta. To uključuje sljedeće [4], [12], [13]:

- Plaćanja vanjskim IT konzultantima: Ovaj trošak obuhvaća sva plaćanja IT stručnjacima izvan organizacije u kojoj se dogodio incident za pružanje stručnih usluga u svrhu rješavanja incidenta. To može uključivati naknade za usluge, troškove putovanja ili druge srodne troškove povezane s angažmanom vanjskih stručnjaka.
- Plaćanja napadačima: U nekim slučajevima, žrtve kibernetičkih napada mogu se odlučiti platiti otkupninu napadačima kako bi povratili pristup svojim podacima ili usluzi. Ovaj trošak obuhvaća iznos novčanih sredstava ili drugih oblika plaćanja koji su preneseni napadačima u zamjenu za povrat ukradenih podataka.

- Ukraden novac: Kada su financijske institucije ili pojedinci žrtve napada usmjerenih na krađu novca, ovaj trošak uključuje iznos ukradenog novca koje je neposredno prenesen s računa žrtve na račun napadača.

2.2. Dugoročni izravni troškovi

Dugoročni izravni troškovi obuhvaćaju sva financijska plaćanja koja su izvršena nakon incidenta. To uključuje sljedeće [4], [12], [13]:

- Plaćanja vanjskim IT konzultantima: Ovaj trošak uključuje angažman stručnjaka izvan organizacije kako bi se izvršila detaljna procjena sigurnosnih propusta i provele revizije sustava. Takvi stručnjaci mogu pružiti preporuke i rješenja za poboljšanje sigurnosti te pružiti stručno znanje i podršku za implementaciju tih rješenja. To može uključivati naknade za identifikaciju potencijalnih rizika ili obuku zaposlenika kako bi se povećala svijest o sigurnosnim praksama.
- Trošak nabave novog ili nadogradnju postojećeg softvera ili sustava: Ovaj trošak uključuje obnovu fizičke imovine odnosno zamjenu oštećenih dijelova te obnovu ili reprodukciju izgubljenih, oštećenih, ukradenih, izbrisanih ili šifriranih podataka ili softvera.
- Trošak zapošljavanja: Ovaj trošak uključuje zapošljavanje novog osoblja kako bi se poboljšala sigurnost i odgovor na incidente. To može uključivati plaće stručnjaka za sigurnost, troškove obuke novih zaposlenika, preraspodjelu odgovornosti unutar organizacije i slično.
- Trošak pravnih naknada: Ovaj trošak uključuje sve pravne troškove koji su povezani s incidentom. To može uključivati angažiranje odvjetnika za savjetovanje, zastupanje organizacije u sudskim postupcima, sudske nagodbe, administrativne postupke i druge pravne aktivnosti koje mogu biti potrebne za rješavanje pitanja koja proizlaze iz sigurnosnog incidenta.
- Troškovi osiguranja: Ovaj trošak obuhvaća premiju osiguranja koju organizacija plaća kako bi pokrila gubitke. To može uključivati troškove osiguranja od kibernetičkih prijetnji ili drugih oblika osiguranja koja pružaju zaštitu od potencijalnih gubitaka [7].

- Novčane kazne ili odštete: Ova stavka uključuje sve novčane kazne ili odštete koje organizacija može biti dužna platiti kao posljedicu sigurnosnog incidenta. To može uključivati novčane kazne koje propisuju regulatorna tijela, naknade štete žrtvama ili troškove izvan sudskih nagodbi kako bi se riješile pravne posljedice incidenta.

2.3. Neizravni troškovi

U neizravne troškove ubraja se sljedeće [4], [12], [13]:

- Trošak radnog vremena zaposlenika: Ovaj trošak obuhvaća vrijeme koje zaposlenici troše izvan svojih redovnih poslova kako bi istražili, analizirali i riješili probleme nastale uslijed sigurnosnog incidenta.
- Vrijednost izgubljenih datoteka: Ova stavka obuhvaća financijsku vrijednost izgubljenih ili oštećenih datoteka ili podataka kao rezultat sigurnosnog incidenta. To može uključivati gubitak vrijednih informacija, osjetljivih podataka o klijentima ili poslovnim procesima.
- Vrijednost gubitka intelektualnog vlasništva: Ovaj trošak podrazumijeva financijsku vrijednost koja proizlazi iz gubitka ili kompromitiranja intelektualnog vlasništva.
- Trošak gubitka poslovanja: Ova stavka obuhvaća financijske gubitke koji proizlaze iz prekida poslovanja. To može uključivati gubitak prihoda zbog nedostupnosti usluga ili smanjenje prodaje proizvoda ili usluga.
- Reputacijski troškovi: Ovaj trošak odnosi se na negativne učinke sigurnosnog incidenta na ugled organizacije. To može uključivati smanjenje povjerenja kupaca, smanjenje vrijednosti dionica na tržištu, gubitak poslovnih partnera ili investitora te dodatne marketinške ili PR napore kako bi se obnovio ugled organizacije.
- Gubitak izvora financiranja: Ova stavka obuhvaća financijski gubitak organizacije zbog povlačenja investitora, donatora ili smanjenja financijske podrške nakon sigurnosnog incidenta. To može uključivati smanjenje priljeva kapitala, otkazivanje ugovora ili smanjenje potencijalnih sredstava za daljnje poslovanje i razvoj.

- Gubitak klijenata: Ovaj trošak obuhvaća gubitak postojećih ili potencijalnih kupaca ili klijenata. To može uključivati smanjenje prodaje, otkazivanje ugovora, gubitak povjerenja kupaca ili smanjenje potražnje za proizvodima ili uslugama organizacije.

2.4. Problemi procjene određenih vrsta troškova

Troškovi koji nastaju kao posljedica incidenta mogu biti podložni utjecaju vanjskih čimbenika. Važno je razlikovati udio troška koji se može izravno pripisati incidentu od vanjskih čimbenika koji također mogu utjecati na procjenu troška [4], [6]. Na primjer, incident može imati učinak na cijenu dionice organizacije, no istovremeno mogu postojati i drugi čimbenici koji utječu na cijenu dionice, a nisu nužno povezani s incidentom. Dakle, na troškove mogu utjecati vanjski čimbenici koji nisu povezani s incidentom kao na primjer opća tržišna nestabilnost, politički faktori, promjene zakonskih propisa i slično. Stoga je prilikom procjene ukupnih troškova povezanih s incidentom, važno pažljivo analizirati i izolirati izravne troškove koji su specifično vezani uz incident od vanjskih čimbenika.

Postoji metodološki izazov u određivanju koji se troškovi trebaju uključiti u precizan izračun ukupnih troškova povezanih s incidentom, a koji ne [4], [9], [10]. Važno je pažljivo procijeniti svaki od navedenih troškova i donijeti odluku o njihovom uključivanju u izračun ukupnog troška incidenta. U središtu takve rasprave nalaze se sljedeći troškovi:

- Troškovi emocionalne štete: To su troškovi koji proizlaze iz emocionalne i psihološke traume koju su doživjeli pojedinci ili organizacija kao rezultat incidenta. Ovi troškovi mogu uključivati liječenje, savjetovanje ili druge oblike podrške za oporavak.
- Troškovi povezani s rješavanjem pritužbi korisnika: Kada se incident odražava na korisnike ili klijente organizacije, mogu se javiti pritužbe ili zahtjevi za nadoknadu prouzročene štete.
- Oportunitetni troškovi radnog vremena osoblja: Prekid uobičajenih aktivnosti uslijed incidenta može zahtijevati angažman zaposlenika organizacije na rješavanju incidenta umjesto na redovne zadatke. Oportunitetni troškovi

odnose se na izgubljenu produktivnost ili vrijeme koje je zaposlenicima bilo potrebno da se vrate svojim uobičajenim zadacima.

- Troškovi pružanja zaštite korisnicima nakon incidenta: Nakon incidenta, organizacija može poduzeti dodatne mjere kako bi zaštitila svoje korisnike ili klijente od daljnjih šteta.
- Povećanje troškova premije osiguranja: Incidenti mogu rezultirati povećanjem troškova premije osiguranja organizacije. To se može dogoditi zbog povećanog rizika ili veće izloženosti organizacije prema budućim potencijalnim incidentima.
- Gubitak investitora, donatora ili financiranja: Incident može utjecati na povjerenje investitora, donatora ili drugih izvora financiranja, što može dovesti do gubitka financijske podrške.
- Gubitak kupaca ili klijenata: Ovaj trošak uključuje gubitak postojećih kupaca ili klijenata kao i potencijalnih novih kupaca ili poslovnih prilika.

Uz diskusiju o tome koji troškovi trebaju biti uključeni u izračun, postoji niz troškova koji se ne mogu precizno izračunati u novčanom smislu [4]:

- Emocionalni troškovi: Incidenti mogu uzrokovati emocionalnu štetu za zaposlenike organizacije. To može uključivati stres, tjeskobu i smanjenu produktivnost. Ovi troškovi odnose se na dobrobit i moral zaposlenika te se ne mogu mjeriti novčano.
- Troškovi reputacije: Incidenti mogu imati negativan utjecaj na reputaciju organizacije, što može rezultirati nepovjerenjem među pojedinim zaposlenicima. Ovaj trošak se odnosi na narušene radne odnose, lošu atmosferu i smanjenu motivaciju što predstavlja izazov u njihovoj procjeni.
- Trošak organizacijskog opreza: Nakon incidenta, organizacija može postati opreznija prema rizicima i odlučiti se ne ulagati u nove tehnologije ili napustiti postojeće tehnologije koje su povezane s incidentom. Strah od ponovnog incidenta može dovesti do povećanih troškova opreza i opreznijeg pristupa poslovanju. Ovaj trošak također nije jednostavan za izračunati.

Iako se ovi troškovi ne mogu precizno izračunati, njihov utjecaj na organizaciju ne bi se trebao zanemariti. Važno je da organizacija svjesno pristupi analizi svih

prethodno spomenutih troškova i njihovom upravljanju kako bi se osiguralo cjelovito razumijevanje ukupnih posljedica incidenta.

Ne smije se zanemariti ni izazov u procjeni vremenskih troškova u sljedećim aspektima [4]:

- Procjena vremena za rješavanje incidenta: Procjena vremena potrebnog za rješavanje incidenta može biti neizvjesna. Stoga je važno da se odmah nakon incidenta temeljito bilježe svi relevantni podaci kako bi se olakšala procjena troškova.
- Izračun vremenskih troškova za zaposlenike ili suradnike koji nisu plaćeni po satu: U nekim slučajevima, određeni zaposlenici ili suradnici mogu biti plaćeni na temelju drugih kriterija koji nisu satnica. U takvim situacijama, izračun troška vremena u satima može biti složen.
- Oportunitetni trošak vremena u odgovoru na incident: Postavlja se pitanje kako konceptualizirati oportunitetni trošak vremena koje osoblje provodi u odgovoru na incident. Potrebno je odlučiti hoće li vrijeme biti tretirano kao trošak ili će se smatrati kao dio radnog vremena osoblja.

Također, neke procjene troškova nije moguće odrediti odmah, a to uključuje [4]:

- Pravne troškove: Pravni troškovi povezani s incidentom često zahtijevaju dulje vrijeme za obradu. Sudski postupci i druge pravne aktivnosti mogu se protezati kroz dulje razdoblje, što otežava trenutno određivanje točnog iznosa troška.
- Gubitak intelektualnog vlasništva i konkurentnosti: Stvarni gubitak intelektualnog vlasništva i konkurentske prednosti često se može uočiti tek u budućim godinama. Utjecaj incidenta na dugoročne aspekte poslovanja zahtijeva vremenski okvir kako bi se pravilno procijenio. Trošak povezan s gubitkom intelektualnog vlasništva nosi određenu razinu nesigurnosti. Iz tog razloga, važno je utvrditi kako se određuje gubitak konkurentske prednosti.
- Gubitak usluga koje nisu izravno povezane sa stvaranjem prihoda: Incidenti mogu rezultirati gubitkom određenih usluga ili funkcionalnosti koje nisu izravno povezane s generiranjem prihoda. Ove vrste gubitaka mogu biti teške za procijeniti jer njihov utjecaj može biti dugoročan.

3. Cyber Conflict Simulator

Cyber Conflict Simulator (CCS) je važan alat koji organizacijama omogućuje da bolje razumiju svoju mrežnu infrastrukturu, procijene rizike i razviju vještine za efikasnu obranu od kibernetičkih prijetnji bez rizika za stvarne sustave i podatke organizacije. Unutar CCS simulatora dostupne su mreže organizacija, omogućujući sudionicima da simuliraju različite napade i isprobaju različite strategije obrane. Svaki korak i odluka koju sudionici donose u okviru simulacije imaju utjecaj na razvoj događaja i rezultate. U ovom poglavlju je opisana mreža organizacije koja se koristi za simulaciju napada i obrane u kontekstu izračunavanja štete nastale uslijed napada. Organizacija koja je odabrana za simulacije napada i obrane je napravljena po uzoru na organizaciju Hrvatski operator prijenosnog sustava d.d. (HOPS d. d.) [30].

3.1. Opis korištene topologije za simulacije napada i obrane

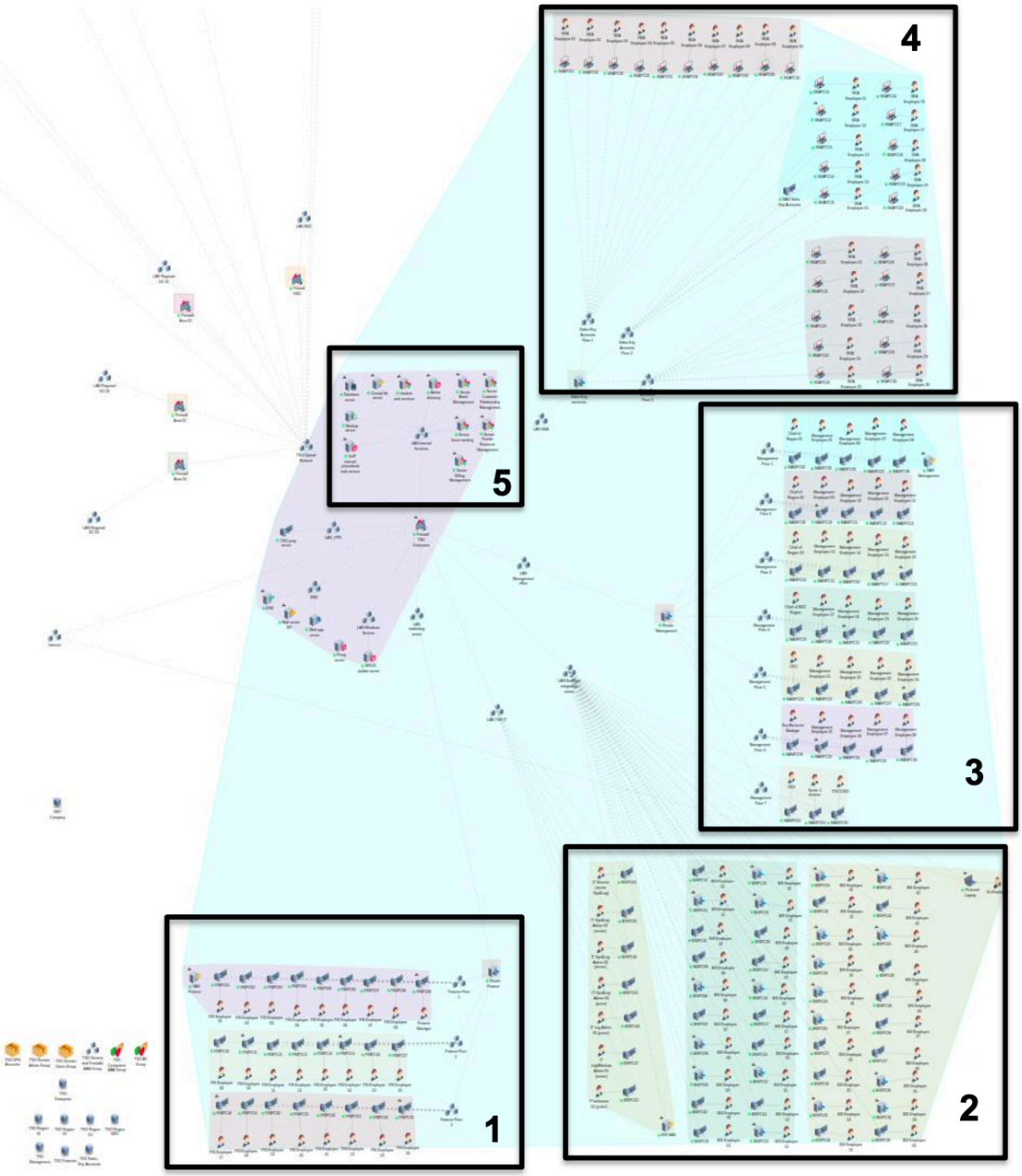
U ovom potpoglavlju pruža se detaljan opis osnovnih pojmova koji su potrebni za razumijevanje mreže organizacije koja se proučava. Prvo je važno razumjeti osnovnu strukturu elektroenergetskog sustava. Elektroenergetski sustav sastoji se od tri komponente :

1. Elektrane koje proizvode električnu energiju.
2. Prijenosni sustav koji preuzima električnu energiju iz elektrana i prenosi je na velike udaljenosti.
3. Distribucijski sustav koji preuzima energiju iz prijenosnog sustava i distribuira ju potrošačima.

Dakle, električna energija se prenosi od proizvođača do potrošača kroz dva sustava: prijenosni sustav i distribucijski sustav. Tim dvama sustavima upravljaju različite tvrtke, općenito poznate kao operator prijenosnog sustava (engl. *Transmission System Operator* - TSO) i operator distribucijskog sustava (engl. *Distribution System Operator* - DSO). Ključna zadaća TSO-a je održavanje ravnoteže u električnom sustavu, što znači da proizvedena energija odgovara potrošenoj energiji.

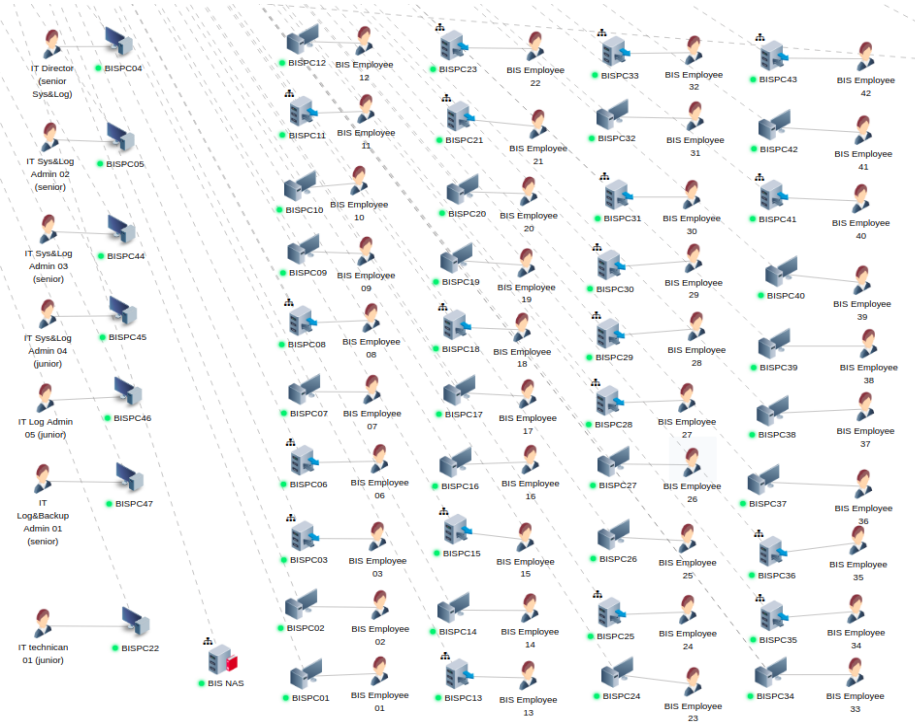
TSO se može podijeliti na poslovni i upravljački dio. Poslovni dio čine četiri odjela koji koriste korporativnu IT mrežu (engl. *information technology - IT*) (Slika 3.1):

- U pravokutniku broj 1 nalazi se *Finance sector (FIN)*
- U pravokutniku broj 2 nalazi se *Business integration sector (BIS)*
- U pravokutniku broj 3 nalazi se *Managment department (MAN)*
- U pravokutniku broj 4 nalazi se *Sales Key Account sector (SKA)*
- U pravokutniku broj 5 nalaze se LAN interne usluge

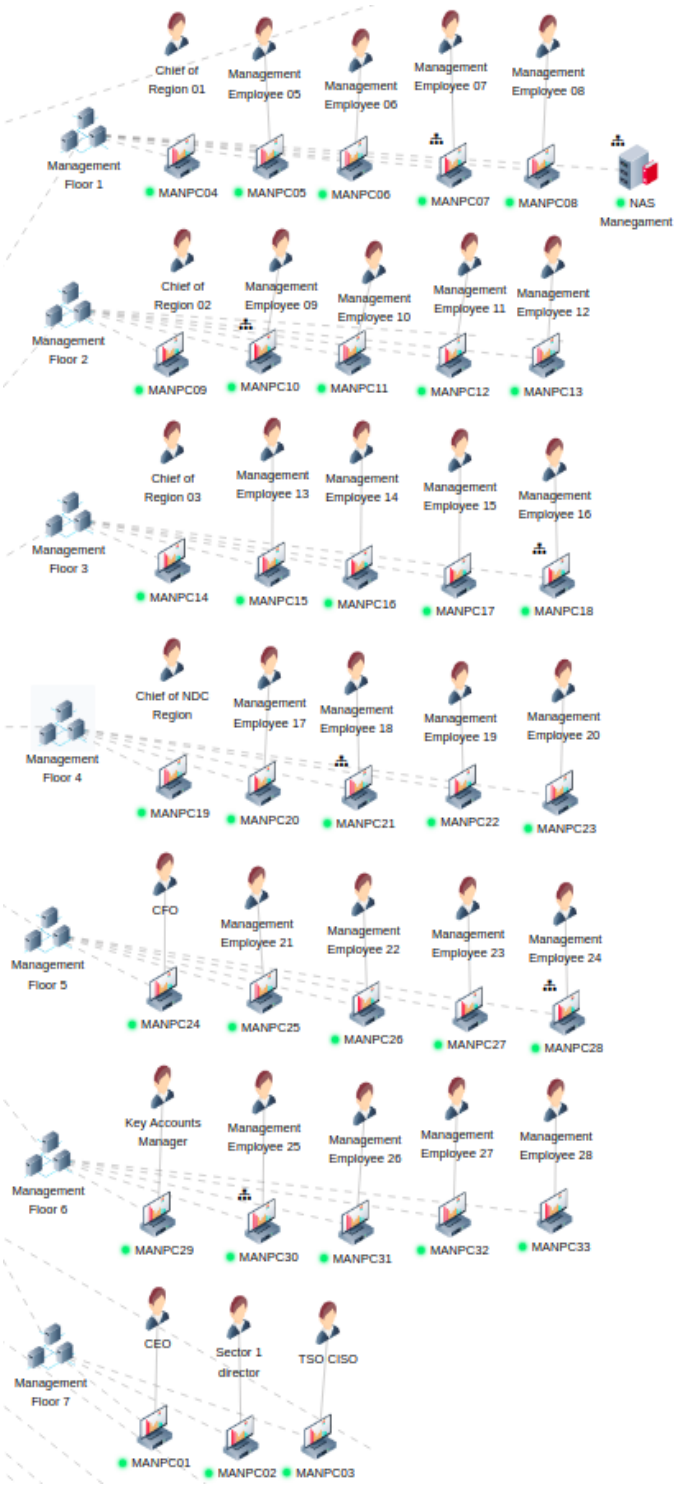


Slika 3.1 Pojednostavljena korporativna IT mreža

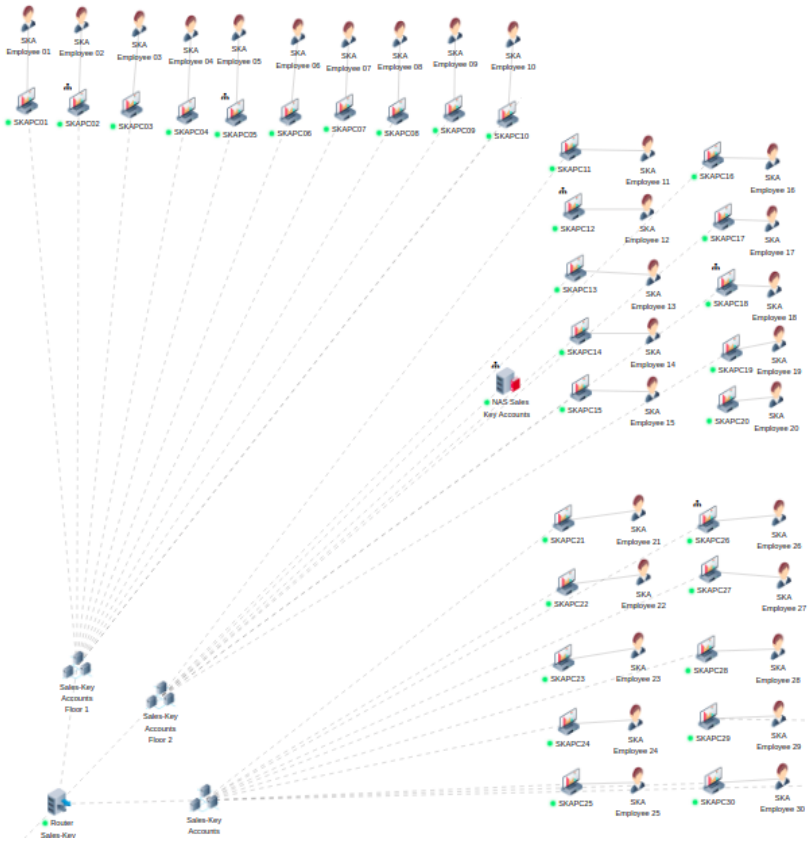
Slika 3.2 *Finance sector (FIN)*



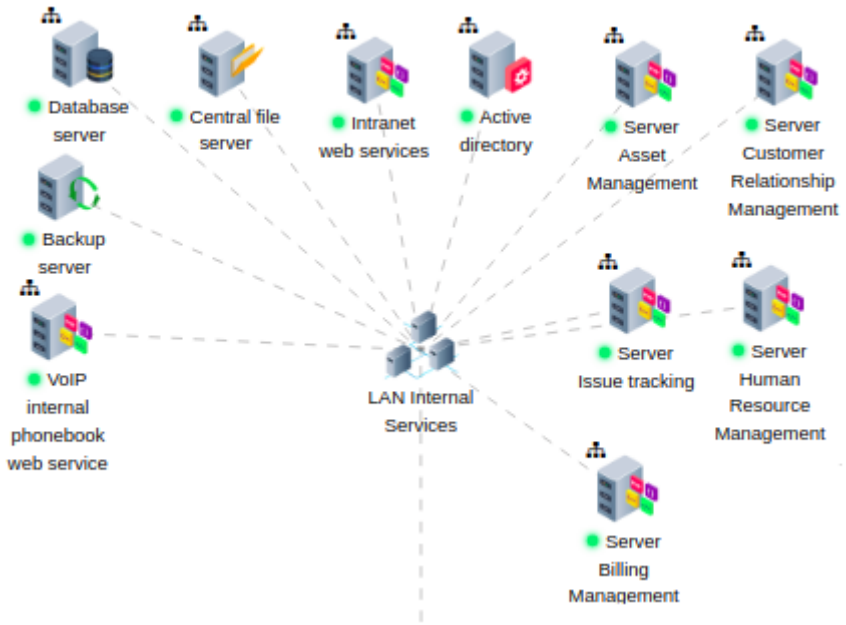
Slika 3.3 *Business integration sector (BIS)*



Slika 3.4 *Managment department (MAN)*



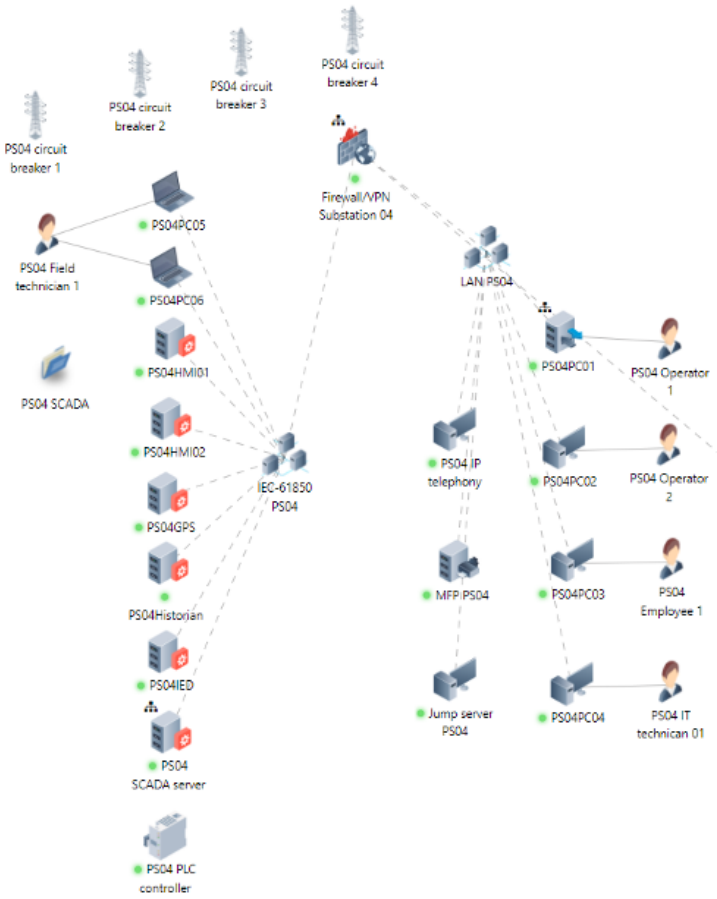
Slika 3.5 *Sales key account sector (SKA)*



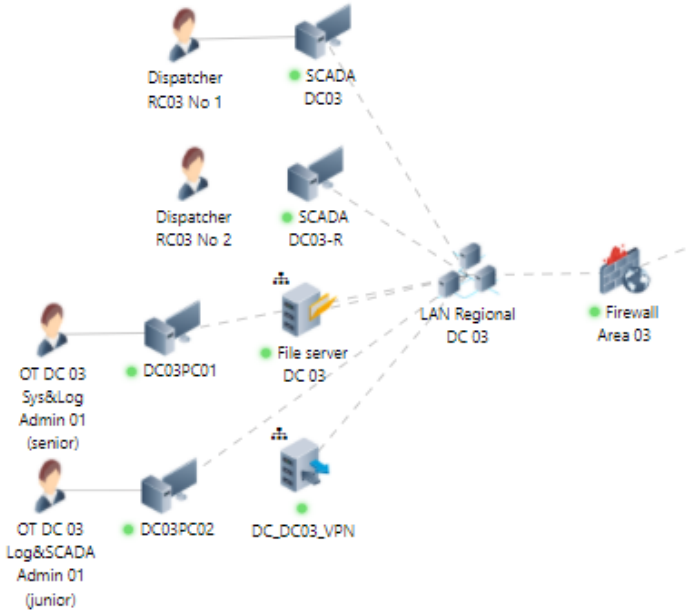
Slika 3.6 LAN interne usluge

Većina odjela je podijeljena u više podmreža, obično na temelju katova. Mreža je segmentirana, što znači da pojedinačnim segmentima nije dopuštena izravna komunikacija, ali unatoč tome mogu pristupiti nekim zajedničkim uslugama kao što je na primjer pristup poslužitelju elektroničke pošte. IT tim odgovoran je za ispravan rad svih usluga od kojih je jedna pristup internetu u cijeloj organizaciji. Sve sumnjive elektroničke poruke se prijavljuju IT timu. IT tim raspolaže sa određenim brojem zaposlenika koji posjeduju vještine analize logova, upravljanja sustavom i sigurnosnog kopiranja, što je važno u kontekstu obrane. Primarni resurs u IT mreži su podaci pa je sigurnosni zahtjev povjerljivosti ovdje najbitniji. Načelo povjerljivosti orijentira se na zaštitu informacija od neovlaštenog pristupa ili otkrivanja. Načelo povjerljivosti uključuje mjere poput šifriranja, kontrole pristupa kako bi se održala povjerljivost osjetljivih podataka. Svaki korisnik u mreži između ostalog ima svoje računalo i adresu elektroničke pošte.

Upravljački dio TSO-a naziva se OT mreža (engl. *operational technology - OT*). OT mreža sastoji se od Nacionalnog dispečerskog centra (engl. *National dispatch center – NDC*) u Zagrebu i mrežnih centara upravljanja u Rijeci, Splitu, Osijeku i Zagrebu. Svaki od mrežnih centara odgovoran je za upravljanje trafostanicama smještenih na području cijele Hrvatske [31]. U osnovi, trafostanica se sastoji od transformatora koji transformira električnu energiju na željenu razinu napona i pripadajuće opreme za upravljanje, nadzor i zaštitu (Slika 3.7). S druge strane, glavna odgovornost upravljačkog centra je siguran prijenos i distribucija električne energije uz održavanje ravnoteže između proizvodnje i potrošnje (Slika 3.8). Upravljački centri opremljeni su SCADA sustavom koji omogućuje kontinuirani nadzor. OT tim ima osoblje sa vještinama upravljanja sustavima, analize logova i SCADA administratore koji su odgovorni za navedene sustave. Proizvodnja i potrošnja uvijek moraju biti gotovo jednake. U slučaju kriznih situacija ili napada na sustav, postoje određene razine mjera koje se mogu poduzeti, pri čemu je krajnja opcija isključivanje trafostanice ili određenih dijelova sustava. S obzirom na to da OT mreža kontrolira nešto u fizičkom svijetu, raspoloživost je ovdje najvažniji sigurnosni zahtjev. Raspoloživost se odnosi na to da usluge koje upravljački sustav kontrolira budu uvijek dostupne korisnicima.



Slika 3.7 Trafostanica



Slika 3.8 Regionalni upravljački centar

4. Određivanje ekonomske štete

U analizi kibernetičkog incidenta, razumijevanje i precizno određivanje ekonomske štete omogućuje procjenu utjecaja štete na organizaciju i donošenje informiranih odluka u vezi s kibernetičkom sigurnošću. S obzirom na opisane poteškoće u procjeni pojedinih troškova iz drugog poglavlja, u određivanju štete neće se uključiti svi navedeni troškovi zbog prethodno opisanih problema. Za izračun ukupnog troška primijenit će se pristup opisan u nastavku teksta.

U kontekstu procjene ukupnog troška u kibernetičkom incidentu, fokus se stavlja na akcije koje poduzimaju osobe tijekom i nakon incidenta. Akcije se temelje na simulacijama obrane koje se izvode u CCS-u. Formula za izračun ukupne štete će biti izvedena kao suma različitih vrsta troškova, pri čemu će neki od njih biti automatski izračunati od strane CCS-a. Ukupna šteta bit će izražena u eurima.

Glavna formula za izračun ukupnog troška temelji se na trošku radnog vremena po zaposleniku organizacije. Dakle, trošak radnog vremena se dobiva množenjem utrošenog vremena u satima za provedbu određene akcije obrane s cijenom satnice zaposlenika.

U skladu s glavnom formulom, dodaju se sljedeći troškovi, uzimajući u obzir vrstu napada koji se dogodio:

- Sva plaćanja vanjskim IT konzultantima: Ovaj trošak odnosi se na uslugu od strane zaposlenika vanjskih organizacija specijaliziranih za IT konzultacije u svrhu pružanja obrambenih mjera protiv napada. Ovo je trošak radnog vremena IT stručnjaka koji se izračunava množenjem utrošenog vremena u satima za trajanje svake akcije s cijenom satnice IT stručnjaka. Osim toga, ako postoji putovanje od točke A do točke B, putni troškovi se dodaju kao umnožak duljine putovanja i cijena putnih troškova po kilometru.

- Plaćanja napadačima: Ovaj trošak odnosi se na vrijednost plaćene otkupnine ili bilo koje druge financijske transakcije izvršene napadaču.
- Trošak gubitka poslovanja: Ovaj trošak obuhvaća izgubljenu zaradu koju bi ugašena usluga ostvarila za vrijeme kada je bila nedostupna, a izračunava se kao umnožak vremena trajanja prekida i cijene zarade po satu koju bi usluga inače ostvarivala. Ovaj trošak će automatski biti izračunat od strane CCS-a na temelju korištene topologije i djelatnosti organizacije.
- Vrijednost izgubljenih datoteka: Ova stavka obuhvaća financijsku vrijednost izgubljenih ili oštećenih podataka. Ovaj trošak može uključivati i iznos ukradenog novca koji je neposredno prenesen s računa žrtve na račun napadača.
- Troškovi sigurnosnih mjera nakon napada: Trošak ljudi za oporavak od napada se računa kao umnožak broja ljudi, cijene radnog vremena po satu i broj sati rada. Kupnja premije osiguranja je trošak koji predstavlja cijenu police osiguranja ako se organizacija odluči osigurati za buduće incidente ili vrijednost police osiguranja koju je organizacija platila prije incidenta kako bi pokrila gubitke. Trošak treniranja zaposlenika uključuje cijenu tečaja za trening po osobi pomnoženu s brojem zaposlenika koji se treniraju te cijenu najma opreme i prostora za trening.
- Trošak nabave novog ili nadogradnju postojećeg softvera ili sustava: Ovaj trošak uključuje cijenu obnove fizičke imovine odnosno obnovu izbrisanih, oštećenih ili šifriranih podataka ili softvera. Navedeni trošak računa se kao konkretna vrijednost uništene fizičke imovine ili kao trošak radnog vremena osobe koja je obavljala zamjenu ili obnovu ili zbroj navedene dvije stavke. Za izračun troška radnog vremena, potrebno je pomnožiti utrošeno vrijeme s cijenom satnice.
- Trošak pravnih naknada, kazni i odšteta: Ovaj trošak uključuje angažiranje odvjetnika, sudske troškove i sve novčane kazne ili odštete koje organizacija može biti dužna platiti kao posljedicu sigurnosnog incidenta.
- Reputacijski trošak: Navedeni trošak uključuje obavijest o napadu i poboljšanje ugleda organizacije u javnosti. Trošak se sastoji od cijene rada tima za odnose s javnošću koja se dobiva množenjem utrošenog vremena tima s cijenom radnog sata.

- Trošak gubitka klijenata: Ovaj trošak računa se kao razlika između broja klijenata u godini prije napada i broja klijenata u godini nakon napada, pomnožena s prihodom koji se ostvaruje od jednog klijenta.

4.1. Opis napada

Napadi na organizacije mogu imati ozbiljne posljedice i uzrokovati značajnu štetu. U nastavku slijedi opis jednog od takvih napada koji uključuje *spear phishing*, zlonamjerni kod i krađu osjetljivih podataka. Redoslijed napada po izvršenim akcijama na organizaciju u ovom scenariju je sljedeći :

1. Napadač preuzima kontrolu nad web poslužiteljem. Na tom poslužitelju nalazi se web aplikacija koja se koristi za pristup računima e-pošte. Međutim, aplikacija je zaražena zloćudnim kodom koji napadač koristi u svrhu daljnjeg napada.
2. Napadač zatim provodi istraživanje kako bi otkrio potencijalne mete. Pomoću različitih tehnika, napadač otkriva računala zaposlenika organizacije, prikuplja njihove podatke, uključujući adrese e-pošte.
3. Napadač pažljivo izrađuje i šalje personalizirane *spear phishing* poruke elektroničke pošte svakoj ciljanoj osobi. Ovakve poruke su namijenjene isključivo određenim metama i sadrže zavaravajući sadržaj kako bi ih se privuklo da otvore i kliknu na poveznicu koja vodi do zaražene web aplikacije.
4. Ciljane osobe otvaraju primljene poruke i ovisno o svijesti o sigurnosti mogu pročitati dobivenu poruku ili kliknuti na poveznicu što dovodi do aktiviranja zloćudnog koda na njihovim računalima.
5. Nakon što određene osobe kliknu na poveznicu, zloćudni kod se preuzima na njihova računala i napadač tada ima mogućnost udaljenog pristupa i upravljanja tim računalima. To omogućuje napadaču izvršavanje različitih aktivnosti s ciljem prikupljanja osjetljivih podataka.
6. Prvo, napadač skenira mrežu organizacije kako bi identificirao druga računala i povezane sustave. To omogućuje napadaču stjecanje boljeg uvida u arhitekturu mreže i identifikaciju potencijalnih ciljeva za daljnje napade. Nadalje, napadač analizira konfiguraciju zaraženog računala kako bi pronašao ranjivosti i slabosti u sigurnosnim postavkama. Napadač također koristi metodu snimanja svih unesenih tipki na zaraženom računalu. Pomoću ove metode napadač ima mogućnost

bilježenja i krađe autentifikacijskih podataka kao što su korisnička imena i lozinke, što omogućuje neovlašteni pristup korisničkim računima. *Command and Control* (C&C) poslužitelj služi napadaču za koordinaciju napada. Napadač koristi C&C poslužitelj za slanje *spear phishing* poruka elektroničke pošte, preusmjeravanje na zaraženu web stranicu te nakon što uspije ukrasti osjetljive podatke, prenosi ih na spomenuti poslužitelj. C&C poslužitelj služi kao posrednik, a koristi se kako bi napadač prikrio svoje tragove te kako bi se omogućila centralizirana kontrola i koordinacija napada.

7. Na kraju napada, napadač je uspješno ukrao dokumente koji su vezani za SCADA konfiguraciju i radne ugovore.

4.2. Procjene troškova korištenih u izračunu

Po završetku napada, napadač ima pristup dvjema datotekama u kojima su SCADA konfiguracije i radni ugovori. SCADA sustavi koriste se za nadzor i upravljanje industrijskim procesima. U SCADA konfiguracijskim datotekama mogu se nalaziti podaci o postavkama i parametrima nadzornih sustava. Ti podaci mogu sadržavati informacije o arhitekturi sustava, postavkama sigurnosti, identifikacijskim podacima i drugim tehničkim detaljima relevantnim za SCADA sustave. S druge strane, radni ugovori obično sadrže informacije o zaposlenicima, njihovim ulogama, odgovornostima, plaćama, ugovornim obvezama i drugim povezanim informacijama. Ti podaci mogu uključivati osobne identifikacijske podatke kao što su imena, adrese, detalji o plaćanju i slično.

U kontekstu specifične organizacije koja se koristi u ovom scenariju, u nastavku je opis korištenih procjena za troškove iz formule koji će biti korišteni za prethodno opisani napad. Specifične brojke poput cijene radnog sata i ostalih, su preuzete iz relevantnih izvora dostupnih na internetu :

- Trošak radnog vremena zaposlenika u definiranoj organizaciji koji rade na obrani: Cijena satnice zaposlenika u organizaciji koja se bavi SCADA sustavima može varirati ovisno o različitim čimbenicima kao što su zemlja, regija, industrija, razina iskustva i uloga u organizaciji. Prosjek je 50 eura po satu [22].

- Sva plaćanja IT konzultantima: Prosječna cijena rada IT stručnjaka iznosi otprilike 55 eura po satu [21]. Važno je napomenuti da ova cijena može varirati ovisno o različitim faktorima kao što su iskustvo, specijalizacija, geografska lokacija, složenost projekta i drugi čimbenici.
- Trošak gubitka poslovanja: Ovaj trošak se temelji na sigurnosnom zahtjevu raspoloživosti. U simulatoru CCS provjerava se status određenih dijelova sustava kako bi se utvrdilo jesu li oni aktivni i povezani s mrežom. Ako se utvrdi da nisu, tada se izračunava trošak gubitka poslovanja koji bi taj dio sustava inače generirao da je bio uključen.
- Vrijednost izgubljenih datoteka: SCADA konfiguracije mogu biti posebno vrijedne u sektorima kao što su energetika i proizvodnja, gdje bi njihova zloupotreba mogla imati ozbiljne posljedice. Na crnom tržištu pronađen je primjer u kojem je pristup velikoj poslovnoj infrastrukturi prodan za približno 20 000 eura [27]. Iako ova cijena može biti povezana s vrijednošću dokumenta SCADA konfiguracije, važno je napomenuti da je ova procjena samo približna, a stvarna cijena može varirati ovisno o potražnji na crnom tržištu. Na temelju informacija iz ukradenih radnih ugovora, možemo pretpostaviti da su među ukradenim podacima informacije o kreditnim karticama zaposlenika. Prema dostupnim izvorima na internetu, prosječna cijena takvih podataka na crnom tržištu za jednu osobu iznosi oko 40 eura [19].
- Troškovi sigurnosnih mjera nakon napada: Prema pronađenim informacijama, utvrđeno je da cijena satnice za stručnjaka za sigurnost koji provodi sigurnosne mjere nakon napada iznosi prosječno 60 eura po satu [21]. U ovom specifičnom incidentu kojeg razmatramo, stručnjak može obavljati zadatke kao što su stvaranje novih korisničkih računa za one koji su bili kompromitirani te instalacija novog sigurnosnog softvera. Važno je napomenuti da se cijene mogu razlikovati ovisno o različitim faktorima, kao što su geografska lokacija, iskustvo stručnjaka, specifične potrebe obnove i drugi relevantni čimbenici. Prosječna godišnja premija za kibernetičko osiguranje iznosi 1500 eura za pokriće od 1 000 000 eura uz franšizu 10 000 eura [24]. Ta premija odnosi se na pokriće od 1 000 000 eura, što znači da osiguravajuće društvo snosi trošak do tog iznosa u slučaju incidenta. Međutim postoji franšiza od 10 000 eura, što znači da osiguranik prvo mora snositi troškove do tog iznosa prije nego što

osiguravajuće društvo počne plaćati naknadu. Naravno, organizacije mogu plaćati znatno manje ili više za svoje osiguranje ovisno o nekoliko ključnih čimbenika kao što su veličina organizacije, priroda njenih poslovnih aktivnosti, rizicima kojima je izložena te raznim drugim. Prosječni trošak programa obuke zaposlenika iznosi oko 60 eura po zaposleniku godišnje [25].

- Trošak kazne: Kazne i pravne posljedice mogu se primijeniti ako organizacija nije uskladila svoje poslovanje s relevantnim zakonima o zaštiti podataka ili ako nije poduzela odgovarajuće sigurnosne mjere kako bi spriječila ili smanjila rizik od kibernetičkih napada te ako je prešutjela napad. Dosad najveća izrečena kazna u Republici Hrvatskoj bila je oko 330 000 eura zbog nepoduzimanja odgovarajućih tehničkih i organizacijskih mjera koje su rezultirale neovlaštenim pristupom osobnim podacima oko sto tisuća građana [26]. U odabranom scenariju u kojem se koristi izuzetno bitna organizacija, može se pretpostaviti da bi prosječna kazna za krađu osobnih podataka zaposlenika iznosila oko 150 000 eura.
- Reputacijski trošak: Troškovi angažiranja tima za odnose s javnošću za obavještavanje o napadu iznose minimalno 1500 eura [28]. Važno je napomenuti da ova procjena obuhvaća samo troškove angažiranja tima za odnose s javnošću koji izrađuju objave za medije i ne uključuje dodatne troškove koji mogu nastati.

4.3. Izračun štete za varijacije obrane

U ovom potpoglavlju opisana su tri različita scenarija u kojima se mijenjaju načini obrane i analiziraju pripadajući troškovi kako bi se procijenila konačna šteta u svakom scenariju. Za svaki scenarij, detaljno su opisane promjene u strategiji obrane, uključujući implementaciju dodatnih sigurnosnih mjera, angažman vanjskih stručnjaka, edukaciju osoblja, primjenu novih programskih rješenja i slično.

CCS simulator generira Excel tablicu nakon svake provedene simulacije. U ovoj tablici detaljno su prikazani vremenski okviri svake akcije koju su zaposlenici poduzeli kako bi se obranili od napada, kao i broj zaposlenika koji su sudjelovali u tim aktivnostima. U sklopu ovog rada, priložene su Excel tablice koje sadrže simulacije napada i obrane. Unutar tablica nalaze se ispisi koji će biti navedeni u opisima koji slijede.

U prvom scenariju, detaljno je opisan tijek obrane uključujući sve korake i postupke koji su poduzeti zbog napada. Također bit će analiziran svaki korak i njegova učinkovitost u smanjenju štete. U drugom i trećem scenariju fokus će biti na promjenama u strategiji obrane i njihovom utjecaju na štetu. Na taj način, pružit će se pregled različitih pristupa i strategija koje su korištene u obrani od napada te njihova uspješnost u smanjenju štete i zaštiti organizacije.

4.3.1. Prvi scenarij obrane

Određeni zaposlenici primili su *spear phishing* poruke elektroničke pošte te su imali mogućnost prijaviti sumnjivu poruku ili kliknuti na poveznicu unutar nje. U ovom scenariju, neki od zaposlenika prijavili su sumnjivu poruku elektroničke pošte. Analizom tih poruka utvrđeno je da poveznice vode prema nesigurnoj web stranici. Primjer ispisa analize jedne od sumnjivih poruka (Ispis 5.1):

```
„E-mail contains a link 'http://webmail.forumofthemall.hr/mail/loging.php' to
                a website 'Webmail SquirrelMail Popular Forum'“
```

Ispis 4.1 Izvješće analize sumnjive poruke elektroničke pošte

U idućem koraku provjerava se da li je bilo koji od zaposlenika kliknuo na poveznicu. U skladu s tim, sljedeći korak uključuje analizu poslužitelja elektroničke pošte s ciljem utvrđivanja je li još neki zaposlenik primio sumnjivu poruku, ali ju nije prijavio. Postoji određeni broj takvih poruka, a njihovom analizom također je otkriveno da poveznice unutar njih vode prema nesigurnoj web stranici.

Provodi se analiza računala zaposlenika koji su kliknuli na poveznice kako bi se pronašli potencijalni indikatori kompromitacije. Iz sljedećeg primjera ispisa, indikator kompromitacije upućuje na mogućnost prisutnosti zloćudnog koda na jednom od računala zaposlenika (Ispis 5.2):

```
    „Suspicious files: 'Irfan View x64' matched indicators of compromise
'ig11ha2pč87ds4gpf6gq' on 'SKAPC17'. 'SKAPC17' added to list of machines in
                focus“
```

Ispis 4.2 Izvješće analize

Na svim računalima na kojima su identificirani indikatori kompromitacije, provodi se detaljnija analiza koja otkriva prisutnost maliciozne datoteke i kompromitacije korisničkih računa. Sljedeći korak je analiza zloćudnog koda, odnosno postupak reverznog inženjerstva kako bi se pokušali saznati ciljevi napadača. S obzirom na obim posla i nedostatak adekvatnog broja zaposlenika za istovremeno izvršavanje svih potrebnih zadataka, angažirat će se vanjska organizacija u svrhu obavljanja reverznog inženjerstva i forenzike. U suradnji s IT stručnjacima vanjske organizacije, cilj je ukloniti zloćudni kod sa zaraženih računala, instalirati sigurnosne nadogradnje, obnoviti kompromitirane korisničke račune te upozoriti zaposlenike na *phishing.* Kao rezultat napada, napadači su uspjeli izvršiti krađu i objaviti važne dokumente o SCADA sustavima kao i dokumente o radnim ugovorima (Ispis 5.3) :

```
„Succssfully sold 50 units of 'Confidential Contracts Information'“,
„Successfully published 'SCADA Configuration'“
```

Ispis 4.3 Izvješće o uspješno izvršenoj krađi podataka

U skladu s navedenom obranom, šteta se u ovom scenariju izračunava prema formuli (1). U ovom scenariju, organizacija je angažirala vanjske IT stručnjake kako bi riješila probleme nastale uslijed incidenta te poduzela sve potrebne mjere za uklanjanje zloćudnih kodova i zaštitu od potencijalnih budućih napada. Stoga se u izračunu ukupne štete ne uzimaju u obzir potencijalne kazne.

$$\begin{aligned} \text{Šteta} = {} & T(\text{radno\_vrijeme\_zaposlenika}) + \\ & T(\text{radno\_vrijeme\_IT\_konzultanata}) + T(\text{gubitak\_poslovanja}) + \\ & T(\text{vrijednost\_izgubljenih\_podataka}) + T(\text{reputacija}) \end{aligned} \tag{1}$$

Osim toga, pretpostavka je da se organizacija nije odlučila osigurati policom osiguranja niti provesti obuku zaposlenika, smatrajući da su poduzete mjere dovoljne za zaštitu. Excel tablice koriste se kao izvor podataka koji se potom koriste za popunjavanje odgovarajućih parametara u formuli za izračun štete. Iz tablice se dobivaju informacije o trajanju svake akcije koje se gledaju kao radno vrijeme osoblja koje je sudjelovalo u obrani. Radno vrijeme se izračunava kao umnožak broja sati rada i cijene satnice. Radno vrijeme zaposlenika koji su sudjelovali u obrani se izračunava prema izrazu (2). Radno vrijeme IT stručnjaka izračunava se prema izrazu (3). Također, parametri u formuli uključuju procjene koje su detaljno opisane na početku ovog poglavlja.

$$T(\text{radno\_vrijeme\_zaposlenika}) = \text{utrošeno\_vrijeme [h]} \times \text{cijena\_satnice [€]} = 38 \text{ [h]} \times 50 \text{ [€]} = 1900 \text{ [€]} \quad (2)$$

$$T(\text{radno\_vrijeme\_IT\_konzultanata}) = \text{utrošeno\_vrijeme [h]} \times \text{cijena\_satnice [€]} = 12 \text{ [h]} \times 55 \text{ [€]} = 660 \text{ [€]} \quad (3)$$

Trošak gubitka poslovanja kojeg računa CCS preuzet je iz Excel tablice. Trošak gubitka poslovanja naveden je pod izrazom (4).

$$T(\text{gubitak\_poslovanja}) = 20\,021 \text{ [€]} \quad (4)$$

Vrijednost izgubljenih datoteka je određena prema procjeni opisanoj na početku poglavlja [19], [27]. Vrijednost izgubljenih datoteka navedena je pod izrazom (5).

$$T(\text{vrijednost\_izgubljenih\_podataka}) = \text{vrijednost\_SCADA\_dokumenata [€]} + 50 \times \text{vrijednost\_osobnih\_podataka [€]} = 20\,000 \text{ [€]} + 50 \times 40 \text{ [€]} = 22\,000 \text{ [€]} \quad (5)$$

Troškovi angažiranja tima za odnose s javnošću za obavještavanje o napadu iznose minimalno 1500 eura [28]. Reputacijski trošak naveden je pod izrazom (6).

$$T(\text{reputacija}) = 1500 \text{ [€]} \quad (6)$$

Uvrštavanjem svih prethodnih izraza u formulu (1), dobiva se šteta u iznosu od 46 081 eura.

$$\text{Šteta} = 1900 \text{ [€]} + 660 \text{ [€]} + 20\,021 \text{ [€]} + 22\,000 \text{ [€]} + 1500 \text{ [€]} = 46\,081 \text{ [€]} \quad (7)$$

4.3.2. Drugi scenarij obrane

U ovom scenariju, organizacija se odlučila za obranu od napada koristeći isključivo interne resurse i osoblje. Redoslijed obrane isti je kao u prvom scenariju, ali s nekoliko novih elemenata. Organizacija je provela osnovne mjere obrane koje su dovele do otkrivanja zlćudnog koda na računalima zaposlenika. Nakon otkrivanja, poduzete su mjere za uklanjanje zlćudnog koda sa zaraženih računala, obnovu korisničkih računa,

upozorenje zaposlenika o *phishing* porukama elektroničke pošte te isključenje određenih dijelova sustava koji su bili kompromitirani. Također su provedeni koraci za sanaciju određenih sigurnosnih propusta koji su omogućili napad. U ovom slučaju, organizacija nije angažirala vanjske IT stručnjake za pomoć. Šteta se u ovom scenariju izračunava prema formuli (8).

$$\text{Šteta} = T(\text{radno\_vrijeme\_zaposlenika}) + T(\text{kazna}) + T(\text{gubitak\_poslovanja}) + T(\text{vrijednost\_izgubljenih\_podataka}) \quad (8)$$

Radno vrijeme zaposlenika koji su sudjelovali u obrani izračunava se prema izrazu (9).

$$T(\text{radno\_vrijeme\_zaposlenika}) = \text{utrošeno\_vrijeme [h] x cijena\_satnice [€]} = 29\ [\text{h}] \times 50\ [€] = 1450\ [€] \quad (9)$$

Organizacija je u ovom scenariju odlučila isključiti znatno veći broj kompromitiranih računala iz svoje mreže što ovdje rezultira većim troškom gubitka poslovanja kojeg računa CCS. Trošak gubitka poslovanja naveden je pod izrazom (10).

$$T(\text{gubitak\_poslovanja}) = 128\ 299\ [€] \quad (10)$$

Organizacija je odlučila zadržati informacije o napadu kako bi zaštitila ugled. Reputacijski trošak i radno vrijeme IT konzultanata neće biti uključeni u izračun budući da organizacija nije koristila njihove usluge. Međutim, budući da je organizacija prešutjela napad i imajući u vidu važnost ovakve organizacije može se uzeti u obzir kazna koju bi dobila zbog nedovoljne zaštite, što je rezultiralo krađom osobnih podataka zaposlenika. Iznos kazne naveden je pod izrazom (11).

$$T(\text{kazna}) = 150\ 000\ [€] \quad (11)$$

Vrijednost izgubljenih datoteka je određena prema procjeni opisanoj na početku poglavlja [19], [27]. Vrijednost izgubljenih datoteka navedena je pod izrazom (12).

$$T(\text{vrijednost\_izgubljenih\_podataka}) = \text{vrijednost\_SCADA\_dokumenata [€]} + 50 \times \text{vrijednost\_osobnih\_podataka [€]} = 20\ 000\ [€] + 50 \times 40\ [€] = 22\ 000\ [€] \quad (12)$$

Uvrštavanjem svih prethodnih izraza u formulu (8), dobiva se šteta u iznosu od 301 749 eura.

$$\text{Šteta} = 1450\ [€] + 150\ 000\ [€] + 128\ 299\ [€] + 22\ 000\ [€] = 301\ 749\ [€] \quad (13)$$

4.3.3. Treći scenarij obrane

U skladu s prethodnim scenarijima, organizacija je poduzela sve temeljne mjere koje su dovele do otkrivanja zloćudnih kodova. S ciljem uklanjanja tih kodova, provođenja reverznog inženjerstva, forenzike i instaliranja nove sigurnosne podrške, angažirala se vanjska organizacija. Zahvaljujući temeljitoj pripremi za obranu, može se pretpostaviti da organizacija nije dobila kaznu. Šteta se u ovom scenariju izračunava prema formuli (14).

$$\begin{aligned}\text{Šteta} = {} & T(\text{radno\_vrijeme\_zaposlenika}) + T(\text{radno\_vrijeme\_IT\_konzultanata}) + \\ & T(\text{gubitak\_poslovanja}) + T(\text{vrijednost\_izgubljenih\_podataka}) + T(\text{reputacija}) + \\ & T(\text{premija\_osiguranja}) + T(\text{obuka\_zaposlenika})\end{aligned} \quad (14)$$

Radno vrijeme zaposlenika i IT konzultanata računa se na standardni način kao i do sada. Radno vrijeme zaposlenika koji su sudjelovali u obrani se izračunava prema izrazu (15). Radno vrijeme IT stručnjaka izračunava se prema izrazu (16).

$$\begin{aligned}T(\text{radno\_vrijeme\_zaposlenika}) &= \text{utrošeno\_vrijeme [h]} \times \\ &\text{cijena\_satnice [€]} = 22\ [h] \times 50\ [€] = 1100\ [€]\end{aligned} \quad (15)$$

$$\begin{aligned}T(\text{radno\_vrijeme\_IT\_konzultanata}) &= \text{utrošeno\_vrijeme [h]} \times \\ &\text{cijena\_satnice [€]} = 26\ [h] \times 55\ [€] = 1430\ [€]\end{aligned} \quad (16)$$

Uz navedene mjere, organizacija je odlučila angažirati i tim za odnose s javnošću kako bi informirala medije o napadu i time očuvala svoj ugled. Troškovi angažiranja tima za odnose s javnošću za obavještavanje o napadu iznose minimalno 1500 eura [28]. Reputacijski trošak naveden je pod izrazom (17).

$$T(\text{reputacija}) = 1500\ [€] \quad (17)$$

Uz to, organizacija je prepoznala važnost ulaganja u osiguranje koje će pružiti dodatni sloj zaštite u slučaju budućih sigurnosnih incidenata. Iznos premije osiguranja naveden je pod izrazom (18).

$$T(\text{premija\_osiguranja}) = 1500\ [€] \tag{18}$$

Nadalje, organizacija je odlučila uložiti resurse u godišnju obuku svojih zaposlenika kako bi ih educirala o sigurnosnim aspektima i opasnostima te osigurala da su dobro pripremljeni za suočavanje s budućim napadima. Ovaj trošak prikazan je izrazom (19).

$$T(\text{obuka\_zaposlenika}) = \text{broj\_zaposlenika x godišnja\_cijena\_obuke}\ [€] = 195 \text{ x } 60\ [€] = 11\ 700\ [€] \tag{19}$$

Vrijednost izgubljenih datoteka navedena je pod izrazom (20), a gubitak poslovanja kojeg računa CCS naveden je pod izrazom (21).

$$T(\text{vrijednost\_izgubljenih\_podataka}) = \text{vrijednost\_SCADA\_dokumenata}\ [€] + 50 \text{ x vrijednost\_osobnih\_podataka}\ [€] = 20\ 000\ [€] + 50 \text{ x } 40\ [€] = 22\ 000\ [€] \tag{20}$$

$$T(\text{gubitak\_poslovanja}) = 29\ 290\ [€] \tag{21}$$

Uvrštavanjem svih prethodnih izraza u formulu (14), dobiva se šteta u iznosu od 68 520 eura.

$$\text{Šteta} = 1100\ [€] + 1430\ [€] + 29\ 290\ [€] + 22\ 000\ [€] + 1500\ [€] + 1500\ [€] + 11\ 700\ [€] = 68\ 520\ [€] \tag{22}$$

4.3.4. Usporedba rezultata

U tablici (Tablica 4.1) prikazani su rezultati, odnosno izračunate štete u tri scenarija opisana u prethodnim potpoglavljima.

U prvom scenariju su poduzete sve temeljne mjere kako bi se riješili problemi uzrokovani incidentom. U obrani su sudjelovali zaposlenici i IT stručnjaci vanjske organizacije. Organizacija je odlučila da neće ulagati u dodatne sigurnosne mjere

nakon napada, smatrajući da su poduzete mjere dovoljne za zaštitu. Iz tog razloga, izračun štete za prvi scenarij je manji u usporedbi s izračunima u drugom i trećem scenariju.

U drugom scenariju organizacija se branila od napada koristeći isključivo interne resurse. Pretpostavljeno je da je dobila veliku kaznu zbog krađe vrlo važnih podataka pa je izračun štete u ovom scenariju znatno veći u usporedbi s izračunom u prvom i trećem scenariju.

U trećem scenariju, u obrani su sudjelovali zaposlenici i IT stručnjaci vanjske organizacije. Također, provele su se sve preventivne mjere uključujući ugovaranje police osiguranja, obuka zaposlenika, sigurnosne zakrpe i slično. Iz tog razloga, izračun štete u trećem scenariju je veći od izračuna štete u prvom scenariju zbog značajnih financijskih izdataka nakon incidenta, ali manji od izračuna štete u drugom scenariju budući da nema visoke kazne.

Rezultati ukazuju na važnost adekvatne pripreme, suradnje i ulaganja u sigurnosne mjere kako bi se smanjile potencijalne štete uzrokovane sigurnosnim incidentima.

Tablica 4.4 Prikaz izračuna šteta

Broj scenarija	**Izračunata šteta [€]**
1	46 081
2	301 749
3	68 520

5. Zaključak

U sklopu ovog rada pružen je pregled troškova koji mogu nastati kao posljedica sigurnosnog incidenta, kao i metodologija za izračunavanje ukupne štete. Kroz primjenu različitih strategija obrane, koristeći definiranu formulu, izračunate su štete u tri scenarija u kojima je napad ostao nepromijenjen, a obrana se mijenjala. Organizacija je obvezna poduzeti sve mjere s ciljem prvotnog otkrivanja i razumijevanja napada kao i rješavanje problema putem uklanjanja zloćudnog koda kako bi se postigao oporavak od napada. Te aktivnosti mogu obavljati interni zaposlenici ili vanjska organizacija. U situacijama kada je potrebno istovremeno obavljati zadatke ili kada interni zaposlenici nisu dovoljno stručni za određene zadatke, nužno je angažirati vanjske IT stručnjake radi postizanja brže i kvalitetnije obrade svih koraka. U obje situacije, organizacija je dužna platiti usluge osoblja koje obavlja svoj posao. Odluka o isključenju kompromitiranih računala iz mreže dovodi do velikog troška budući da se time onemogućuje funkcionalnost dijela sustava koji bi inače generirao određeni profit za organizaciju. Ako organizacija propusti poduzeti osnovne mjere obrane, suočit će se s mogućnošću izricanja visoke kazne, s obzirom na to da napadi mogu rezultirati ozbiljnom krađom podataka. Najveći financijski izdaci zapravo dolaze nakon što je napad završen, kroz provedbu preventivnih mjera poput ugovaranja polica osiguranja, ažuriranja softvera, obnove korisničkih računa, primjene sigurnosnih zakrpa i slično. U ovom radu su prikazane procjene troškova temeljene na podacima prikupljenim s interneta, s naglaskom na to da stvarne organizacije računaju s konkretnim podacima kao što su satnice njihovih zaposlenika, sudski troškovi, stvarne vrijednosti plaćanja IT stručnjacima, odvjetnicima i ostalima. Konačni troškovi ovise o vrsti napada, samoj organizaciji, vrsti usluge koju organizacija pruža te razvoju obrane. Unatoč tome, ovaj rad pruža organizacijama mogućnost da dobe koristan uvid u potencijalne štete, temeljem načina na koji mogu reagirati na napad. Za postizanje preciznijeg izračuna štete, preporučuje se uključivanje svih relevantnih troškova unutar simulatora CCS. Dodatno, bilo bi korisno da organizacije popune detaljni upitnik koji sadrži sve relevantne podatke, kao što su satnice zaposlenika i ostali relevantni parametri, koji su neophodni za točno izračunavanje ukupne štete. Na taj način, simulator bi samostalno izračunao ukupnu štetu prema konceptu koji je predstavljen u radu.

6. Literatura

[1] Cyber Conflict Simulator – često postavljana pitanja. Poveznica: https://ccs.utilis.biz/Home/Faq; pristupljeno: 10. svibnja 2023.

[2] European Union Agency for Cybersecurity (2021.), ENISA Threat Landscape 2021. Poveznica: https://www.enisa.europa.eu/publications/enisa- threat-landscape-2021; pristupljeno : 28. listopada 2022.

[3] Agrafiotis, Ioannis, et al. "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate." *Journal of Cybersecurity* 4.1 (2018): tyy006.

[4] Furnell, Steven, et al. "Understanding the full cost of cyber security breaches." *Computer fraud & security* 2020.12 (2020): 6-12.

[5] Riek, Markus, et al. "Estimating the costs of consumer-facing cybercrime: A tailored instrument and representative data for six EU countries." *Workshop on the Economics of Information Security (WEIS), University of California at Berkeley*. Vol. 2. 2016.

[6] Cashell, Brian, et al. "The economic impact of cyber-attacks." *Congressional research service documents, CRS RL32331 (Washington DC)* 2 (2004).

[7] Romanosky, Sasha, et al. "Content analysis of cyber insurance policies: How do carriers price cyber risk?." *Journal of Cybersecurity* 5.1 (2019): tyz002.

[8] Woods, Daniel, et al. "Mapping the coverage of security controls in cyber insurance proposal forms." *Journal of Internet Services and Applications* 8.1 (2017): 1-13.

[9] Gwebu, Kholekile L., Jing Wang, and Wenjuan Xie. "Understanding the cost associated with data security breaches." *PACIS*. 2014.

[10] Wolff, Josephine, and William Lehr. "Degrees of ignorance about the costs of data breaches: What policymakers can and can't do about the lack of good empirical data." *Available at SSRN 2943867* (2017).

[11] How to calculate the cost of a data breach – a case study, CealPath. Poveznica: https://www.sealpath.com/blog/how-to-quantify-the-cost-of-a-data-breach-a-case-study/; pristupljeno: 16. prosinca 2022.

[12] Official Statistics, Cyber Security Breaches Survey 2022 – GOV.UK. Poveznica: https://www-gov-uk.translate.goog/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022?_x_tr_sl=en&_x_tr_tl=hr&_x_tr_hl=hr&_x_tr_pto=sc; pristupljeno: 09. prosinca 2022.

[13] How To Calculate The Cost Of DaTa Breach, Ekran. Poveznica : https://www.ekransystem.com/en/blog/cost-of-a-data-breach; pristupljeno: 23. prosinca 2022.

[14] Haislip, Jacob, et al. "The economic cost of cybersecurity breaches: A broad-based analysis." *Workshop on the Economics of Information Security (WEIS)*. 2019.

[15] Malliouris, D., and A. C. Simpson. "Underlying and consequential costs of cyber security breaches: Changes in systematic risk." Workshop on the Economics of Information Security, 2020.

[16] McGrath, Vincent, Elizabeth A. Sheedy, and Fan Yu. "Governance of Cyber Security: State of Play." *Available at SSRN 3971177* (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] How much is your information worth to a cybercriminal via the Dark Web?, Keeper. Poveznica : https://www.keepersecurity.com/how-much-is-my-information-worth-to-hacker-dark-web.html; pristupljeno: 15. travnja 2023.

[19] Dark Web Price Indeks (2022.), PrivacyAffairs. Poveznica: https://www.privacyaffairs.com/dark-web-price-index-2022/; pristupljeno: 15. travnja 2023.

[20] How Much Is Your Dana Actually Worth?, Cyber Defense Magazine. Poveznica: https://www.cyberdefensemagazine.com/how-much/; pristupljeno: 15. travnja 2023.

[21] Hourly Rate for Skill: Cyber Security, Payscale. Poveznica: https://www.payscale.com/research/US/Skill=Cyber_Security/Hourly_Rate/Page-3; pristupljeno: 15. travnja 2023.

[22] Hourly Wage for SCADA Engineer Salary in the United States, Salary.com. Poveznica: https://www.salary.com/research/salary/recruiting/scada-engineer-hourly-wages; pristupljeno: 15. travnja 2023.

[23] How Much Does Cyber Insurance Cost? Blog Insurance Explained, Embroker. Poveznica: https://www.embroker.com/blog/cyber-insurance-cost/; pristupljeno: 15. travnja 2023.

[24] Cyber Insurance Cost, AdvisorSmith. Poveznica: https://advisorsmith.com/business-insurance/cyber-liability-insurance/cost/; pristupljeno: 15.travnja 2023.

[25] How Much Does Security Awareness Training Cost?, Lascala.com. Poveznica: https://lascala.com/how-much-does-security-awareness-training-cost/; pristupljeno: 15. travnja 2023.

[26] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ, Zakon RH. Poveznica : https://www.zakon.hr/z/3112/Opća-uredba-o-zaštiti-podataka---Uredba-%28EU%29-2016-679-; pristupljeno: 15. travnja 2023.

[27] How much does access to corporate infrastructure cost? Securelist.com. Poveznica: https://securelist.com/initial-access-data-price-on-the-dark-web/106740/; pristupljeno: 15. travnja 2023.

[28] Cjenik PR usluga – kako se kreću cijene agencija za odnose s javnošću u Hrvatskoj, Krešimir Macan (2010., lipanj). Poveznica : https://manjgura.hr/blog/cjenik-pr-usluga-kako-se-krecu-cijene-agencija-za-odnose-s-javnoscu-u-hrvatskoj; pristupljeno: 15. travnja 2023.

[29] Englesko-hrvatski rječnik, Groš S. Poveznica: http://www.zemris.fer.hr/~sgros/stuff/rjecnik.shtml; pristupljeno 23. svibnja 2023.

[30] HOPS d. d., „O nama“. Poveznica: https://www.hops.hr/o-nama; pristupljeno: 23. svibnja 2023.

[31] HOPS d. d., „Model vođenja EES-a“. Poveznica: https://www.hops.hr/model-vodenja-ees-a; pristupljeno: 23. svibnja 2023.

Sažetak

Određivanje ekonomske štete u organizaciji u ovisnosti od načina obrane

Pouzdane procjene ekonomske štete uzrokovane kibernetičkim kriminalom su rijetke. Ovaj rad se bavi problemom izračunavanja ekonomske štete u organizaciji koja je pretrpjela napad, s naglaskom na analizu utjecaja obrambenih strategija na veličinu štete.

Svaka odluka organizacije u provođenju obrane ima značajan utjecaj na ukupnu štetu odnosno financijske izdatke organizacije. U radu se daje pregled svih relevantnih vrsta troškova koji mogu proizaći iz napada što predstavlja koristan temelj za procjene ekonomske štete. Kod izračuna korišten je simulacijski alat *Cyber Conflict Simulator* koji automatski procjenjuje jednu vrstu troškova, dok se ostali pridodaju kako bi se stvorila cjelovita slika. Rezultati analize ukazuju na to da se šteta odražava u gubitku vremena i novčanih sredstava, a troškovi zaštite prije i nakon napada predstavljaju značajne financijske izdatke. Korišteni pristup omogućuje preciznije razumijevanje financijskih posljedica napada te olakšava organizacijama donošenje informiranih odluka o odabiru i primjeni obrambenih strategija utemeljenih na konkretnim podacima.

Ključne riječi: ekonomska šteta, *Cyber Conflict Simulator*, troškovi, kibernetički napad, financijski izdaci, obrambene strategije

Summary

Determining economic damage in an organization based on defense strategies

Reliable estimates of the economic damage caused by cybercrime are rare. This paper addresses the problem of calculating economic damage in an organization that has suffered an attack, with a focus on analyzing the impact of defense strategies on the extent of the damage.

Every decision an organization makes in implementing defense measures significantly affects the overall damage and financial expenditures. The paper provides an overview of all relevant types of costs that may arise from an attack, serving as a valuable foundation for economic damage assessments. The Cyber Conflict Simulator, a simulation tool, was used for calculations, automatically estimating one type of cost, while others were added to create a comprehensive picture. The analysis results indicate that damage is reflected in the loss of time and financial resources, and pre- and post-attack protection costs represent significant financial expenditures. The adopted approach enables a more precise understanding of the financial consequences of attacks, facilitating informed decision-making for organizations regarding the selection and application of defense strategies based on concrete data.

Keywords: economic damage, *Cyber Conflict Simulator*, costs, cyber attack, financial expenditures, defense strategies.

Skraćenice

CCS	*Cyber Conflict Simulator*	simulator kibernetičkih napada
C&C	*Command and Control*	nadzorni poslužitelj
TSO	*Transmission System Operator*	operator prijenosnog sustava
DSO	*Distribution System Operator*	operator distribucijskog sustava
IT	*information technology*	informacijska tehnologija
OT	*operational technology*	industrijska upravljačka tehnologija
PR	*public relations*	odnosi s javnošću
SCADA	*Supervisory Control and Dana Acquisition*	sustav nadzora i upravljanja

Privitak

U privitku ovog rada nalaze se tri Excel tablice koje prikazuju kronološki redoslijed izvođenja simulacija napada i obrane, uključujući sve specifične akcije, kao i ispisane vrijednosti izračunatih troškova generiranih od strane CCS simulatora.