Sveučilište u Rijeci
University of Rijeka
https://www.uniri.hr

Polytechnica: Journal of Technology Education, Volume 6, Number 2 (2022)
Politehnika: Časopis za tehnički odgoj i obrazovanje, Volumen 6, Broj 2 (2022)

Politehnika
Polytechnica
http://www.politehnika.uniri.hr
cte@uniri.hr

DOI: https://doi.org/10.36978/cte.6.2.2

Pregledni članak
Review article
UDK: 004.056
658:004.056

Uvid u kibernetičku sigurnost i obranu: oblikovanje koncepcijskog modela kibernetičke otpornosti

Darko Galinec
Tehničko veleučilište u Zagrebu
Informatičko-računarski odjel
Vrbik 8, 10000 Zagreb
darko.galinec@tvz.hr

Sažetak

Planiranje kibernetičke sigurnosti unutar složenog sustava i primjena njezinih načela i postupaka ima cilj (eng. end) postići otpornost sustava u kibernetičkom prostoru tj. kibernetičku otpornost (eng. Cyber Resilience). Svrha složenoga sustava je izvršavanje misije (zadaće, poslanja) kao skupa sposobnosti i sklonosti s obzirom na unutarnje i vanjske okolnosti sustava. Za postizanje kibernetičke otpornosti potrebna su organizacijska, ljudska, materijalna (tvarna) i financijska (novčana) sredstva (eng. means) u provedbi mjera, aktivnosti i postupaka za smanjenje razine rezidualnog (preostalog) sigurnosnog rizika. To je onaj dio sigurnosnog rizika kojeg je unutar sustava nužno prihvatiti, budući da u trenutku procjene rizika, s obzirom na unutarnje i vanjske okolnosti kao prilika za razvoj sposobnosti, nije moguće postići njegovo daljnje smanjivanje. Koncepcijskim istraživanjem prikazanim u ovom radu analiziraju se načini (eng. ways) i sredstva (eng. means) za postizanje kibernetičke otpornosti u uvjetima rastućih sigurnosnih rizika današnjice. Cilj ovog istraživanja je stvaranje novoga modela kibernetičke otpornosti, koji obuhvaća kibernetičku i informacijsku sigurnost. Kontekst modela čine neprepoznati sigurnosni rizici u kibernetičkom prostoru, a za oblikovanje modela rabi se metoda koncepcijskog modeliranja. Model podrazumijeva i obuhvaća svjesnost o postojanju nepoznatih ranjivosti sustava i istodobno nepoznatih kibernetičkih ugroza (eng. Cyber Threats) i napada (eng. Cyber Attacks) kao mogućih posljedica postojanja neprepoznatih ranjivosti. Pri tome se, također, uzima u obzir činjenica kako su načini sprječavanja do tada neviđenih ugroza i napada nultog dana (eng. Zero-Day Attacks) u velikom broju poslovnih slučajeva danas nepoznati, jednako kao i načini obrane i možebitni odgovori na iste - nepoznate nepoznanice (eng. Unknown Unknowns). Za suočeljavanje s navedenim izazovima postoji potreba za stvaranjem „znanja o neznanju“ složenog sustava tj. za razvojem kibernetičkih sposobnosti i njihovom ostvarenju, temeljem načela kibernetičke sigurnosti i kibernetičke obrane.

Ključne riječi: *atribucija; kibernetička obrana; kibernetička otpornost; kibernetička sigurnost; koncepcijski model.*

1 Uvod

Svrha ovog rada je izrada koncepcijskog modela kibernetičke otpornosti kao sposobnosti složenog sustava u kibernetičkom prostoru. Model je nastao strukturiranjem mjera zaštite informacija (eng. *Information Assurance* - IA) i određivanjem međusobne uvjetovanosti i povezanosti njezinih sastavnica (kibernetičke sigurnosti kao procesa, informacijske sigurnosti kao stanja, kibernetičke

obrane kao postupka i mehanizma). Cilj rada je istražiti ranjivosti, ugroze, prijetnje i rizike koji svakodnevno dolaze iz kibernetičkog prostora, te omogućiti i doprinijeti svjesnosti o potrebi za postizanjem kibernetičke otpornosti složenog sustava, kroz spoznaju ponašanja i međudjelovanja njegovih sastavnica (komponenti). Pri tome je posebno istaknuto upravljanje rizikom: proces koji treba dovesti do smanjenja razine nepoznatosti i neznanosti ponašanja sustava na najmanju moguću mjeru. Za postizanje cilja, postupkom koncepcijskog modeliranja oblikovan je model otpornosti sustava u kibernetičkom prostoru, utemeljen na kriteriju vrste kibernetičke ugroze. To su ugroze povjerljivosti, cjelovitosti i raspoloživosti podatka (eng. *Confidentiality, Integrity and Availability* - CIA), napredne napadačke prijetnje te napadi nultog dana.

Primjenom različitih scenarija, promatranjem ponašanja sustava i usporedbom ishoda model postaje pogodan za određivanje stanja (poznate poznanice, poznate nepoznanice, nepoznate nepoznanice) sustava tijekom kibernetičkih ugroza te odabir strategija djelovanja, a time i potpora odlučivanju o taktikama/akcijama koje treba poduzeti unutar sustava.

Rad je strukturiran kako slijedi: u prvom, uvodnom poglavlju, navode se kibernetička sigurnost, obrana i otpornost kao temeljni pojmovi ovog rada; u drugom poglavlju dan je pregled postojeće literature s temeljnim pojmovima; u trećem poglavlju razmatra se upravljanje rizikom, strategija kibernetičke sigurnosti i atribucija u svrhu postizanja kibernetičke otpornosti; u četvrtom poglavlju razmotrena je kibernetička otpornost i njen kontekst te je prikazan i objašnjen novi koncepcijski model otpornosti, s mogućnostima primjene i mogućim pravcima daljnjeg istraživanja; u petom, zaključnom poglavlju, prikazana su konačna razmatranja i zaključak rada.

U novije vrijeme Institut za hrvatski jezik i jezikoslovlje, kao središnja je nacionalna znanstvena ustanova za istraživanje hrvatskoga jezika i općega jezikoslovlja predlaže izraz „kiber“, koji se rabi u hrvatskom prijevodu dokumenata Europske unije. U svim postojećim zakonima i pravilnicima RH za to područje, kao i Odlukama Vlade RH o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost (koje je autor teksta jedan od članova) rabi se izraz „kibernetički“. Autor rada se zbog navedenog odlučio za uporabu izraza „kibernetički“.

2 Pregled literature i temeljni pojmovi

Prema Zakonu o informacijskoj sigurnosti (Hrvatski sabor, 2007) pojedini pojmovi u smislu ovoga Zakona imaju sljedeće značenje:

Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda.

Mjere informacijske sigurnosti su opća pravila zaštite podataka koja se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini.

Standardi informacijske sigurnosti su organizacijske i tehničke procedure i rješenja namijenjena sustavnoj i ujednačenoj provedbi propisanih mjera informacijske sigurnosti.

Područja informacijske sigurnosti predstavljaju podjelu informacijske sigurnosti na pet područja s ciljem sustavne i učinkovite realizacije donošenja, primjene i nadzora mjera i standarda informacijske sigurnosti.

Sigurnosna akreditacija informacijskog sustava je postupak u kojem se utvrđuje osposobljenost tijela i pravnih osoba za upravljanje sigurnošću informacijskog sustava, a provodi se utvrđivanjem primijenjenih mjera i standarda informacijske sigurnosti.

Prema objavi na službenim stranicama (Središnji državni ured za razvoj digitalnog društva, 2022) kibernetička sigurnost obuhvaća skup procesa, mjera i standarda kojima se jamči određena razina pouzdanosti pri korištenju proizvoda i usluga u kibernetičkom prostoru, pri čemu sustavna zaštita računala i računalnih mreža, informatičke i informacijske infrastrukture, mobilnih uređaja i podataka od malicioznih napada značajno pridonosi, odnosno, sve aktivnosti koje su nužne za zaštitu od kibernetičkih ugroza mrežnih i informacijskih sustava, korisnika tih sustava i drugih osoba na koje one utječu.

Kibernetičku ugrozu predstavlja svaka moguća okolnost, događaj ili djelovanje koji bi mogli oštetiti, poremetiti ili na drugi način negativno utjecati na mrežne i informacijske sustave, korisnike tih sustava i druge osobe.

U okviru informacijsko-komunikacijska tehnologije (IKT) razlikujemo:

- proizvod IKT-a - element ili skupina elemenata mrežnih i informacijskih sustava;
- usluga IKT-a - koja se u cijelosti ili uglavnom sastoji od prijenosa, pohranjivanja, preuzimanja ili obrade informacija s pomoću mrežnih i informacijskih sustava;
- proces IKT-a - skup aktivnosti koje se provode radi oblikovanja, razvoja, ostvarivanja ili održavanja IKT proizvoda ili IKT usluge;

U vremenu ubrzanog razvoja novih tehnologija i digitalizacije društva područje kibernetičke sigurnosti ima sve veći značaj i bilježi snažan globalni rast zbog

permanentnog oslanjanja društva u cjelini na umrežavanje i korištenje informacijskih sustava. Vlada Republike Hrvatske je također prepoznala značaj ovog područja te postavila strategijski okvir za kibernetičku sigurnost kroz Nacionalnu strategiju kibernetičke sigurnosti i Akcijski plan za njezinu provedbu. Upravo ti dokumenti su temelj za provedbu svih aktivnosti s ciljem zaštite svih korisnika suvremenih elektroničkih usluga, kako u javnom i gospodarskom sektoru, tako i među građanstvom u cjelini. Krajnji cilj je uređen, dostupan, otvoren i siguran hrvatski kibernetički prostor kroz koordiniran i uravnotežen odgovor niza institucija koje predstavljaju sve sektore društva.

Kibernetičke prijetnje bilježe kontinuirani porast na globalnoj razini, a različite vrste napada u kibernetičkom prostoru postaju sve sofisticiranije i složenije i utječu na naš svakodnevni život i poslovanje. Različiti maliciozni programi, računalne prijevare, zloporabe osobnih i financijskih podataka te zloporabe na društvenim mrežama samo su neki od njih. Upravo iz toga razloga vrlo je bitna svijest o mogućim kibernetičkim ugrozama i kako se od njih zaštititi.

2.1 Kibernetička sigurnost i kibernetički prostor

Prema Nacionalnoj strategiji kibernetičke sigurnosti (Vlada Republike Hrvatske, 2015.) kibernetički prostor je prostor unutar kojeg se odvija komunikacija između informacijskih sustava. U kontekstu Strategije obuhvaća Internet i sve sustave povezane na njega. Kibernetička sigurnost obuhvaća aktivnosti i mjere kojima se postiže povjerljivost, cjelovitost i dostupnost podataka i sustava u kibernetičkom prostoru.

U Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (Hrvatski sabor, 2018) mrežni i informacijski sustav je elektronička komunikacijska mreža, definirana zakonom kojim se uređuje područje elektroničkih komunikacija (a). Također, to je i bilo koji uređaj ili grupa povezanih ili srodnih uređaja, od kojih jedan ili više njih programski izvršava automatsku obradu digitalnih podataka (b) ili digitalni podatci (c) koji se pohranjuju, obrađuju, dobivaju ili prenose prethodno navedenim elementima opisanim u točkama (a) i (b) radi njihova rada, uporabe, zaštite i održavanja.

Sigurnost mrežnih i informacijskih sustava je sposobnost mrežnih i informacijskih sustava da na određenoj razini pouzdanosti odolijevaju bilo kojoj radnji koja ugrožava dostupnost, autentičnost, cjelovitost ili povjerljivost, pohranjenih, prenesenih ili obrađenih podataka, ili srodnih usluga koje ti mrežni i informacijski sustavi nude ili kojima omogućuju pristup. Svojstvo kibernetičke sigurnosti je uporaba Interneta (online), sukladno definicijama kibernetičke sigurnosti i kibernetičkog prostora - preuzeto iz Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN/2018).

„Kibernetička sigurnost je sustav organizacijskih i tehničkih aktivnosti i mjera kojima se postiže autentičnost, povjerljivost, cjelovitost i dostupnost podataka, kao i mrežnih i informacijskih sustava u kibernetičkom prostoru.“

„Kibernetički prostor je virtualni prostor unutar kojeg se odvija komunikacija između mrežnih i informacijskih sustava te obuhvaća sve mrežne i informacijske sustave neovisno o tome jesu li povezani na Internet.“ - preuzeto iz Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN/2018).

Kibernetička sigurnost se, stoga, odnosi na dio kibernetičkog prostora koji po definiciji podrazumijeva mrežnu povezanost (online), uključujući internetski, ali i ma koji drugi mrežni protokol jer „obuhvaća sve mrežne i informacijske sustave“.

2.2 Kibernetička obrana

Ne postoje općeprihvaćene definicije kibernetičkih izraza - oni se rabe u različitim okolnostima i s obzirom na to imaju različita značenja NATO Cyber Cooperative Cyber Defence Center of Excellence (2017). Međutim, Techopedia (2019) daje definiciju i daljnje objašnjenje izraza „kibernetička“ obrana: kibernetička obrana je postupak obrane računalne mreže koji uključuje odgovor na postupke i zaštitu ključne infrastrukture i informacijsko osiguranje za organizacije, vladine organizacije i druge moguće mreže.

Kibernetičku obranu čine sredstva za postizanje i izvršenje obrambenih mjera za suzbijanje kibernetičkih prijetnji i ublažavanje njihovih učinaka, a time očuvanje i vraćanje sigurnosti komunikacija, informacija ili drugih elektroničkih sustava ili podataka koji se pohranjuju, obrađuju ili prenose na te sustave.

Kibernetička obrana se usredotočuje na sprečavanje, otkrivanje i pružanje brzih odgovora na napade i prijetnje tako da ne dođe do promjena na infrastrukturi ili informacijama. S porastom volumena i složenosti kibernetičkih napada, kibernetička obrana je postala ključna za većinu subjekata kako bi se zaštitile osjetljive informacije i čuvala imovina (Galinec, Steingartner, 2017).

Kibernetička obrana pruža prijeko potrebno osiguranje da bi se izvodili procesi i aktivnosti, bez brige o prijetnjama. Ona pomaže u unaprjeđenju korisnosti sigurnosnih resursa i troškova, osobito na ključnim lokacijama. Američko ministarstvo obrane (eng. *Department of Defense* - DOD) je prepoznalo potrebu za ubrzavanjem otkrivanja i odgovora na

zlonamjerne čimbenike u mreži i definiralo novi koncept - aktivna kibernetička obrana (eng. *Active Cyber Defence* - ACD). ACD je sposobnost DOD-a da u stvarnom vremenu otkrije, analizira i umanji prijetnje i slabosti (United States Department of Defense, 2011).

3 Strategija kibernetičke sigurnosti i upravljanje rizikom

Europska unija poduzela je niz mjera kako bi uredila odnose u kibernetičkom prostoru, povećavajući pri tome otpornost i svoju kibernetičku sigurnosnu pripravnost. Od prve strategije EU-a za kibernetičku sigurnost (Europski parlament, 2013), koja je donesena 2013., u kojoj su utvrđeni strategijski ciljevi i konkretne mjere za postizanje otpornosti, smanjenje kibernetičkog kriminaliteta, razvoj politike kibernetičke obrane i sposobnosti za kibernetičku obranu, razvoj industrijskih i tehnoloških resursa i uspostavu usklađene međunarodne politike kibernetičkog prostora za EU, do najnovije iz 2020., u kojoj su dodatno naglašena tri područja - (1) otpornost, tehnološka suverenost i vodstvo, (2) izgradnja operativnih kapaciteta u svrhu sprječavanja, odvraćanja i uzvraćanja, (3) razvijanje globalnog i otvorenog kibernetičkog prostora, stalno se naglašava potreba za reguliranjem digitalne transformacije društva kako bi čovjek uvijek ostao u središtu zbivanja, odnosno subjekt, i u kibernetičkom prostoru, pri čemu je razvidan značaj sigurnosnih parametara za izgradnju povjerenja prema tim procesima.

Radi povećanja povjerenja i sigurnosti na Jedinstvenom digitalnom tržištu Unije (JDT) te s obzirom na brzo širenje povezanih uređaja (internet stvari), bilo je potrebno uspostaviti okvir za sigurnosno certificiranje proizvoda IKT-a, usluga i procesa odnosno svih objekata kibernetičkog prostora.

Navedeno postaje posebno važno, s obzirom na sve veću uporabu kibernetičkih tehnologija, za namjene koje zahtijevaju visok stupanj pouzdanosti i sigurnosti (Hrvatski Sabor, 2021a) te je primjetno povećanje ovisnosti o proizvodima IKT-a, uslugama i procesima, osobito u prometu (automatizirano upravljanje), u sustavima održavanja života i zdravlja (e-zdravstvo), u industriji (kontrolni sustavi za industrijsku automatizaciju - IACS) te u ostvarivanju ljudskih interesa i prava (e-građani). Direktiva o sigurnosti mrežnih i informacijskih sustava („Direktiva NIS"), transponirana Zakonom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, je regulirala razvrstavanje usluga odnosno objekata kibernetičkog prostora po njihovom značaju (ključne usluge i ostale) te uspostavila sustav otpornosti (štićenje, izvješćivanje i interveniranje), specifično za najvažnije sektore (Hrvatski sabor, 2021b). Najnovijim prijedlogom izmjena se planira uvesti preciznije razvrstavanje po značaju i finija raspodjela po još više sektora. Slijednim propisom, koji se na Direktivu NIS i naslanja, Uredbom o ENISA-i te o kibernetičkoj sigurnosnoj certifikaciji (Središnji državni ured za razvoj digitalnog društva, 2021) u području komunikacijske i informacijske tehnologije („Akt o kibernetičkoj sigurnosti") dovršena je druga faza uređivanja kibernetičkog prostora iz aspekta objekata tog prostora. Uredbom je ENISA (Agencija Europske unije za kibernetičku sigurnost) dobila aktivniju i važniju ulogu u postizanju kibernetičke otpornosti Unije te je postala stožerno tijelo u mreži agencija država članica koje se bave kibernetičkom sigurnošću na sličan način. Glavni regulator na razini Europske unije je Europska komisija koja, uz operativnu pomoć ENISA-e i savjetodavnu Europske skupine za kibernetičku sigurnosnu certifikaciju (ECCG - European Cybersecurity Certification Group), osigurava provedbu odredbi oba ova zakona, a sukladno proklamiranim Strategijama i planskim dokumentima.

Jedan od ciljeva postizanja kibernetičke sigurnosti je jačanje Jedinstvenog digitalnog tržišta EU, kako bi ono postalo značajniji čimbenik na globalnoj sceni i postalo otpornije na ometajuća (eng. *disruptive*) djelovanja konkurentskih globalnih gospodarstava. Time se olakšava postizanje i jednog od strategijskih ciljeva Unije - digitalne suverenosti, odnosno mogućnosti slobodnog i samostalnog odlučivanja o svim stvarima u svezi s kibernetičkim prostorom. Posljedično navedenom, države članice EU su preuzele obvezu harmoniziranja svojih propisa i djelovanja na ovom području, te izgradnje ili prilagodbe nacionalnih sustava kibernetičke sigurnosne certifikacije zajedničkom. Očekuje se da sve „nacionalne komponente" u dogledno vrijeme postanu „komponente na nacionalnoj razini" dobro uvezanog i otpornog europskog sustava kibernetičke sigurnosne certifikacije. Kako bi to zaista skladno funkcioniralo, bilo je potrebno odrediti načela i pravila izgradnje sustava kibernetičke sigurnosti, što se Aktom o kibernetičkoj sigurnosti nastojalo i napraviti, a od država članica se očekuje provoditi. Definirane su uloge raznih tijela (Hrvatski Sabor, 2021a), njihovi pravni statusi i načini asociranja, kako bi se postigla ujednačenost komponenata na razini Unije i na kraju izbjeglo štetno fragmentiranje praksi i procedura.

3.1 Suvremeni aspekti kibernetičke sigurnosti

Suvremeni aspekti kibernetičke sigurnosti podložni su brzim promjenama. Brzina, raznolikost i sofisticiranost kibernetičkih napada dramatično se mijenjaju. Mnoge države smatraju kibernetičke sposobnosti, uz diplomaciju, ekonomsku i vojnu moć, dijelom svojih strategijskih alata.

Među najvećim izazovima za kibernetičku obranu nalazi se raznolikost načina na koje se kibernetičke sposobnosti mogu rabiti. Prvo, špijunaža omogućena u kibernetičkom prostoru, bilo na strategijskoj ili operativnoj razini, može ugroziti povjerljivost informacija i informacijskih sustava, potencijalno odajući tajne i osjetljive informacije protivnicima. Drugo, sabotaža omogućena u kibernetičkom prostoru može imati važne fizičke posljedice, pogotovo kada su u pitanju kritične infrastrukture ili manipuliranje podatcima kako bi se unijele zabune i naštetilo ispravnosti odlučivanja i zapovijedanja.

3.2 Atribucija

Atribucija (lat. *attributio*) je pripisivanje ili pridavanje odgovornosti i krivnje za određene uzroke događaja u smislu tko/što ga je prouzročio/prouzročilo.

Uspostavljanje atribucije za kibernetičke operacije je teško, ali ne i nemoguće. Ne postoji jednostavan tehnički proces ili automatizirano rješenje za određivanje odgovornosti za kibernetičke operacije. Brižan, težak rad u mnogim slučajevima zahtijeva tjedne ili mjesece analize inteligencije i forenzike kako bi se procijenila krivnja. U nekim slučajevima, međunarodna zajednica može utvrditi internetsku atribuciju unutar nekoliko sati od incidenta, ali točnost i pouzdanost pripisivanja ovise o dostupnim podatcima.

Svaka vrsta kibernetičke operacije - zlonamjerna ili ne - ostavlja trag. Analitičari rabe ove informacije, zajedno sa svojim znanjem o prethodnim događajima i alatima i metodama poznatih zlonamjernih aktera, pokušavajući pratiti te operacije natrag do njihovih izvora. Analitičari uspoređuju nove informacije s postojećim znanjem, procjenjuju dokaze kako bi odredili razinu pouzdanosti za svoje prosudbe, te razmatraju alternativne hipoteze i nejasnoće za izradu procjena kibernetičke atribucije.

Analitičari mogu ocijeniti odgovornost za kibernetički napad na tri načina:

- prema mjestu porijekla, kao što je određena zemlja;
- prema određenom digitalnom uređaju ili osobi koja se koristi Internetom;
- prema pojedincu ili organizaciji koja je izvršila aktivnost.

Treću kategoriju često je najteže procijeniti jer je nužno povezati zlonamjerne kibernetičke aktivnosti s određenim pojedincima i procijeniti sponzora i motivatore tih pojedinaca.

Pripisivanje napada određenoj zemlji ili akteru zahtijeva prikupljanje što više podataka kako bi se dovelo u vezu aktere online, pojedince i druge entitete. Budući kako to često rezultira stotinama proturječnih pokazatelja, identificiraju se ključni pokazatelji za pravodobnu i točnu atribuciju. To su:

- Namjera: oslanja se na pokazatelje iz vanjskih izvora, kao što su izvješća otvorenih izvora od privatnih tvrtki za kibernetičku sigurnost.
- Ponašanje: u smislu primjene tehnika, metoda i tehnologija, često se rabi za obavljanje kibernetičkog napada ili špijunaže. To je najvažniji pokazatelj jer je teže mijenjati navike od tehničkih alata. Alati, tehnike i postupci napadača mogu otkriti obrasce napada, ali njihov značaj se smanjuje kad postanu javni i drugi ih akteri (eng. *actor)* mogu oponašati.
- Infrastruktura: fizička i / ili virtualna komunikacijska struktura koja se rabi za isporuku kibernetičkih sposobnosti ili za održavanje i kontrolu sposobnosti.
- Zlonamjerni softver: softver oblikovan za omogućavanje neovlaštenih funkcija na kompromitiranom računalnom sustavu, kao što je bilježenje ključa, snimanje zaslona, snimanje zvuka, daljinsko upravljanje i kontrola, te trajni pristup.
- Obveza napadača za izvršavanjem određenih radnji na temelju konteksta. Prikriveni, zanijekani kibernetički napadi često se pokreću protiv protivnika prije ili tijekom regionalnih sukoba ili služe za potiskivanje ili maltretiranje protivničke države.

Pokazatelji iz vanjskih izvora: također se rabe izvješća iz privatne industrije, medija, akademske zajednice i istraživačkih centara kako bi se omogućili takvi podatci ili podijelile hipoteze o počiniteljima.

Najbolje prakse za određivanje atribucije:

- Traženje ljudske pogreške. Gotovo svi uspjesi u davanju internetskih atributa rezultat su otkrivanja i iskorištavanja pogrešaka operativne sigurnosti napadača.
- Pravodobna suradnja, dijeljenje informacija i dokumentacija.
- Strogi analitički pristup.

Prepoznavanje jaza:

U slučajevima kada analitičari nemaju dovoljno podataka za izjavu o prosudbi ili povjerenju u atribuciju jer nema dovoljno pokazatelja, to treba izričito navesti.

4 Kontekst kibernetičke otpornosti

Od početaka razvoja komunikacijske i informacijske tehnologije do danas, odstupanja u njihovom ispravnom radu nastajala su zbog različitih razloga, od ljudskih pogrešaka ili zlonamjernih postupaka, do tehnoloških grešaka ili organizacijskih propusta.

4.1 Kibernetičke sposobnosti

Svi suvremeni aspekti kibernetičke sigurnosti podložni su brzim promjenama. Brzina, raznolikost i sofisticiranost kibernetičkih napada dramatično se

mijenjaju. Mnoge države smatraju kibernetičke sposobnosti, uz diplomaciju, ekonomsku i vojnu moć, dijelom svojih strategijskih alata.

Špijunaža omogućena u kibernetičkom prostoru, bilo na strategijskoj ili operativnoj razini, može ugroziti povjerljivost informacija i informacijskih sustava, potencijalno odajući tajne i osjetljive informacije protivnicima. Drugo, sabotaža omogućena u kibernetičkom prostoru može imati važne fizičke posljedice, pogotovo kada su u pitanju kritične infrastrukture ili manipuliranje podatcima kako bi se dovelo do zabune i onemogućilo odlučivanje i zapovijedanje. MO i OS RH izloženi su, kao i ostali dijelovi društva, cijelom spektru prijetnji iz kibernetičkog prostora.

Imajući to u vidu potrebno je sustavno razvijati sposobnosti kibernetičke obrane temeljem akcijskog plana kojim će biti definirani nositelji pojedinih mjera kao i rokovi, potrebna financijska sredstva te pokazatelji provedbe pojedine mjere.

Mjere za razvoj kibernetičkih sposobnosti mogu se podijeliti na tri područja:

- politika i strategija kibernetičke obrane
- organizacija i sposobnosti kibernetičke obrane
- izobrazba i obuka za kibernetičku obranu.

4.2 Koncepcijski model kibernetičke otpornosti

Svrha novog modela je omogućiti uvid u odnose između informacijske sigurnosti, kibernetičke sigurnosti i kibernetičke otpornosti, sukladno novouvedenom kriteriju vrste ugroza/napada na informacijske sustave, s obilježjem rastuće složenosti.

Za razliku od dotadašnjih promišljanja i zakonskog okvira o odnosima navedenih kategorija, Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (Hrvatski sabor, 2018). u definicijama kibernetičkog prostora i kibernetičke sigurnosti stvara osnovu za omogućavanje uvođenja kriterija mrežne povezanosti (online) s vanjskim sustavima poslovnog sustava te, posljedično, prepoznavanje sofisticiranih mrežnih ugroza/napada, uz do tada već poznate napade CIA koji se nalaze u području informacijske sigurnosti, prepoznate Zakonom o informacijskoj sigurnosti (Hrvatski sabor, 2007). Novost oblikovanog koncepcijskog modela je, nadalje, uvođenje kibernetičke otpornosti kao sposobnosti i krovnog pojma u okviru dane hijerarhije pojmova i vrhovnog cilja čijem postizanju treba, u smislu sigurnosti informacijskog sustava kroz kontinuirano upravljanje rizikom sa svrhom njegova smanjivanja, težiti svaki poslovni sustav današnjice.

Cilj samog novog modela je stvoriti okvir za stvaranje svijesti nositelja odlučivanja područja informacijske i kibernetičke sigurnosti o mogućim rizicima iz unutarnjeg i vanjskog okružja poslovnog sustava. Nadalje, cilj je primjenom novog modela omogućiti razvrstavanje uočenih (poznatih) ili procijenjenih (nepoznatih) vrsta prijetnji prema njihovoj složenosti i utjecaju na stanje sigurnosti informacijskog sustava poslovnog subjekta. Temeljem razvrstavanja i utvrđivanja kategorije određene ugroze/napada te sukladno najboljem znanju, nositelji odlučivanja trebaju odrediti odgovarajuće mjere i postupke te ih kontinuirano provoditi.

Kibernetički rizik (eng. *Cyber Risk*) koji je nužno prihvatiti jer se u trenutku promatranja na njega ne može više djelovati u smislu smanjenja, utvrđuje se procjenom nedostataka rizika/usklađenosti (eng. *Risk/Compliance Gap Assessment*).

Prema autorima rada „Combining Cybersecurity and Cyber Defense to Achieve Cyber Resilience“ (Galinec, Steingartner, 2017) samo kibernetička sigurnost za smanjivanje rizika više nije dovoljna: postoji potreba za strategijom obrane, prevencijom i odgovorom. Ideja otpornosti, u svom osnovnom obliku, je procjena što će se dogoditi prije, tijekom i nakon što mrežno povezani sustav bude suočen s prijetnjom. Otpornost ne bi trebala biti sinonim „oporavku“. Ona nije specifična za događaj, nego dugoročno raste i trebala bi biti uključena u cjelokupnu organizacijsku i poslovnu strategiju. Otpornost u kontekstu sposobnosti sustava i organizacija da izdrže kibernetičke događaje se odnosi na pripreme s obzirom na prijetnje i ranjivosti, obrane koje su postavljene i resursi koji su dodijeljeni za umanjenje sigurnosnih incidenata nakon što se dogode. Ključ je u normalizaciji. Kibernetički rizik se treba promatrati kao bilo koji drugi rizik koji organizacija mora savladati kako bi ispunila svoje ciljeve. Voditelji poslovanja i vlada trebaju razmišljati o otpornosti zbog dva razloga: prvo, na taj način izbjegavaju katastrofalne neuspjehe koji dolaze pristupom „sve ili ništa“, drugo, osiguravaju da razgovor ide dalje od informacijske tehnologije ili informacijske sigurnosti. Prva točka tumači dugoročni pogled i izdržljivost kao ključne čimbenike u osiguravanju kibernetičke otpornosti, što ne treba daljnje objašnjenje. Plan koji obuhvaća djelovanja i rezultate prije, tijekom i nakon pojave prijetnje će biti superioran planu koji razmatra samo jedan faktor u danom trenutku. Druga točka govori o tome da voditelji trebaju proširiti razgovor zaslužuje više pozornosti. Za ekonomsku i društvenu otpornost je ključno razmatranje koje osim informacijske sigurnosti obuhvaća i mrežnu otpornost što osigurava da se možemo nositi s postojećim rizicima i suočiti se s novim rizicima koji će doći s pojavom umjetne inteligencije, IoT-a i kvantnog računarstva. Kako bi se osigurala dugoročna otpornost, organizacije moraju uključiti u strategijsko planiranje sposobnost provedbe

iteracija nad novim prijetnjama iz novih rastućih disruptivnih tehnologija.

Promoviranjem sveukupnog pristupa kibernetičkoj otpornosti, dugoročna strategija (uključujući tehnologije koje će organizacija ugraditi u narednih 10 ili više godina) je kontinuirana strategijska konverzacija koja uključuje i tehnologiju i voditelje u organizaciji. Pristup s kibernetičkom otpornošću osigurava veću spremnost i manje ponavljanja čineći ju, ukupno gledano, učinkovitijom i djelotvornijom. Suprotno od otpornosti, sigurnost se može gledati binarno. Nešto jest ili nije sigurno. Obično je dodijeljeno jednoj, ograničenoj tehničkoj funkciji, držeći neautorizirane korisnike izvan umreženog sustava.

Dok postoje mnoge definicije kibernetičke sigurnosti, postoji razlika između kontrole pristupa i dugoročnog načina razmišljanja, više usmjerenog strategijski, koji kibernetička otpornost treba potaknuti (Galinec, Steingartner, 2017).

Dodatno, s obzirom da ranjivost u jednom području može ugroziti cijelu mrežu, otpornost zahtijeva konverzaciju usredotočenu na sustave umjesto na pojedinačne organizacije. Za umrežene tehnologije, ranjivost u jednom čvoru može utjecati na sigurnost i otpornost čitave mreže. Zbog toga, otpornost je najbolje razmatrati u okviru dobrih „zajedništava". Zbog toga su partnerstva ključna. Ona mogu biti između poslovanja (eng. *business*), regulatora, tužitelja i zakonodavaca. S obzirom da je kibernetička otpornost stvar upravljanja rizikom, ne postoji jedna točka u kojoj počinje ili završava. Umjesto toga, dolazi iz izgradnje strategije i rada na osiguravanju da se mehanizmi transfera rizika koji rade za tradicijske prijetnje mogu nositi s novim kibernetičkim prijetnjama. Odgovornost za kibernetičku otpornost je više pitanje strategije nego taktike. Otpornost zahtijeva da oni na najvišim funkcijama u kompaniji, organizaciji ili vladi spoznaju važnost umanjenja rizika. Iako je osiguravanje veće otpornosti svačija odgovornost, voditelji koji postave strategiju za organizaciju su u konačnici odgovorni i sve više su odgovorni za uključivanje kibernetičke otpornosti u strategiju organizacije. Pravi izazov za kibernetičku sigurnost je ono nepoznato.

Bivši tajnik američkog ministarstva obrane, Donald Rumsfeld je dao objašnjenje ovoga tijekom konferencije za medije 2002. godine: „Postoje poznate poznanice. Postoje stvari koje znamo. Postoje poznate nepoznanice. To jest, postoje stvari za koje znamo da ih ne znamo. Ali također postoje i nepoznate nepoznanice. To su stvari za koje ne znamo da ih ne znamo." (Zak, 2021).

Borba protiv poznatih prijetnji je ključni dio strategije kibernetičke sigurnosti. Ide uz bok naprednim sposobnostima predviđanja, hvatanja i učenja iz nepoznatih prijetnji. Sustavi imaju različite slabe točke i različite procese (izazovi) i oni upravljaju rizikom svaki na svoj način (rješenja). Drugim riječima, svakom sigurnosnom izazovu (procijenjenom kao „poznat" ili „nepoznat") postoji odgovarajuće rješenje. Uključivanjem u model vrijednosti dobivenih tijekom procjene sigurnosti rizika dobivamo „poznate poznanice" koje se odnose na kibernetičku sigurnost i „nepoznate nepoznanice" koje se odnose na kibernetičku otpornost.

Primjer: Postoji poznata kriza u radnoj snazi kibernetičke sigurnosti: golemi nedostatak kvalificiranih i uvježbanih sigurnosnih profesionalaca. Također, postoji i nepoznato rješenje za tu krizu. Široki i rastući doseg izazova zahtijeva i odgovarajuće proširenje skupa vještina koje su i poznate i nepoznate (Galinec, Steingartner, 2017).

Napadači koji stoje iza naprednih napadačkih prijetnji imaju cilj napasti organizacije visoke vrijednosti poput državnih ministarstava, agencija, razvojnih ustanova, obrambenih organizacija i sustava. Prikrivenim napadima na njihove računalne mreže ostvaruju neodobreni pristup istima i ostaju unutar mreže neopaženo kroz duže vremensko razdoblje. APT se uobičajeno odnosi na organizaciju (primjerice vlada) koja ima namjeru, cilj i sposobnost ustrajnog, djelotvornog i učinkovitog napada na određeni cilj. Tehnike i taktike kojima se napadači služe neprestano se razvijaju te kibernetičke ugroze obuhvaćaju nizove zlonamjernih aktivnosti.

Postoje načini na koje se može otkloniti čimbenik straha od nepoznatih veličina, a koji će ih učiniti poznatima. I dalje postoje važni načini da se primjene znanja o poznatim kibernetičkim prijetnjama kako bi sustav kontinuirano bio siguran.

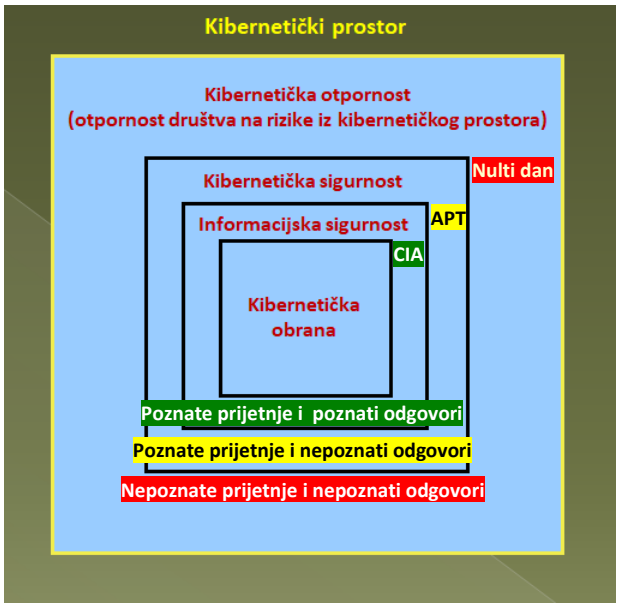
Da bi se nosili s rastućim izazovima koji se danas manifestiraju kao nepoznate nepoznanice, sustavi nastoje osposobiti osoblje i razviti nove procese organizacije i tehnologije. Razvijaju se tehnologije koje, za razliku od tradicijskih pristupa, mogu zaštititi sustav od ozbiljnih prijetnji učenjem što je „normalno" za organizaciju i njezine ljude i na taj način uočiti rastuće anomalije. Za razliku od tradicijskog pristupa s pravilima i otiscima, tehnologija može uočiti prijetnje koje mogu naštetiti organizaciji i mreži, a koje se ne mogu otkriti tradicijskim pristupima. On se može nositi s nesigurnošću i daje prilagodljivu zaštitu za organizacije od unutarnjih prijetnji i vanjskih kibernetičkih napada (Galinec, Steingartner, 2017).

Postupkom koncepcijskog modeliranja, u ovom radu oblikovan je model otpornosti sustava u kibernetičkom prostoru s atribucijom. Polazište raščlambe za oblikovanje i izradu modela jest kriterij vrste kibernetičke ugroze (CIA, APT, nulti dan) složenog sustava. Model je prikazan slikom 1.

Prema autorima rada „Cybersecurity and Cyber Defence: National Level Strategic Approach" (Galinec i sur., 2017) uočavamo i razlikujemo sljedeće pojmove:

Kibernetička otpornost (eng. *Cyber Resilience*): **sposobnost** sustava, organizacije, misije ili poslovnog procesa predviđanja kibernetičkog napada, izdržavanja, oporavka i prilagodbe (adaptacije) svojih sposobnosti pri sučeljavanju s protivnikom u kibernetičkom prostoru (Galinec i sur., 2017).

Informacijska sigurnost (CIA-ino trojstvo prijetnji i odgovor na njih, tj. poznate poznanice), kibernetička sigurnost (ne CIA-ine složene prijetnje, APT-ovi i odgovarajući odgovori tj. poznate nepoznanice) i kibernetička otpornost (nepredvidive prijetnje i odgovori tj. nepoznate nepoznanice) predstavljaju vrste napada kao kriterije prema kojima razlikujemo informacijsku sigurnost s kibernetičkom obranom, kibernetičku sigurnost kao nadskup informacijske sigurnosti te, u konačnici, kibernetičku otpornost kao cilj i nadskup svih prethodno navedenih pojmova. Dodatni argument za poimanje kibernetičke sigurnosti kao nadskupa informacijske sigurnosti daje definicija kibernetičke sigurnosti i kibernetičkog prostora sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (Hrvatski sabor, 2018). Tim definicijama se kibernetička sigurnost odnosi na sigurnost u kibernetičkom prostoru, a kibernetički prostor obuhvaća sve mrežne i informacijske sustave **neovisno o tome jesu li povezani na Internet.**



Slika 1: Koncepcijski model kibernetičke otpornosti

Prema Zakonu o informacijskoj sigurnosti (Hrvatski sabor, 2007), informacijski sustav je komunikacijski, računalni ili drugi elektronički sustav u kojem se podatci obrađuju, pohranjuju ili prenose, tako da budu dostupni i upotrebljivi za ovlaštene korisnike. Područja informacijske sigurnosti za koja se propisuju mjere i standardi informacijske sigurnosti su:

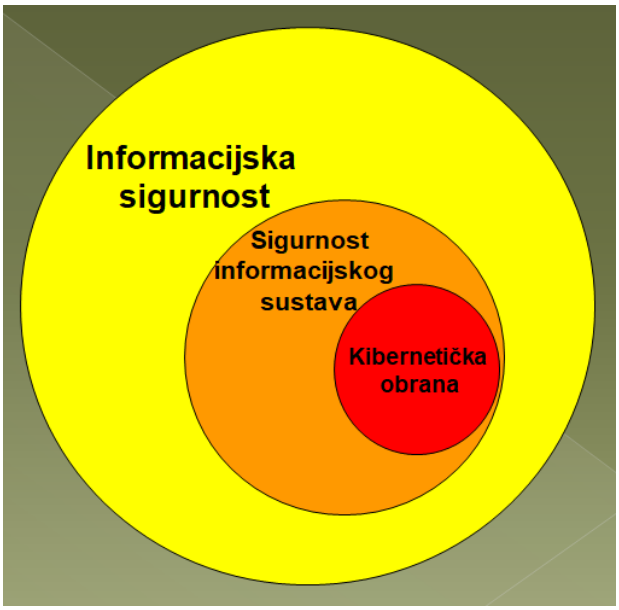
- sigurnosna provjera,
- fizička sigurnost,
- sigurnost podatka,
- **sigurnost informacijskog sustava,**
- sigurnost poslovne suradnje (Hrvatski sabor, 2007).

Sigurnost informacijskog sustava odnosi se na zaštitu komunikacijsko-informacijskog sustava kroz implementaciju mjera i standarda informacijske sigurnosti, a isti uključuje:

- ispunjavanje zahtjeva informacijske sigurnosti,
- sigurnost operacijskih sustava i korisničkih programa i razvoj sigurnosti,
- sigurnosna sustavska arhitektura,
- tehnologijska istraživanja i razvoj u komunikacijsko-informacijskom sustavu,
- planiranje sustavskih zahtjeva za sigurnost,
- testiranje i vrjednovanje,
- razvoj sustava.

Daljnjim uvidom u procese dolazimo do kibernetičke obrane (obrane od prijetnji i rizika koji dolaze **iz kibernetičkog prostora**).

Kibernetička obrana (eng. *Cyber Defence*): mehanizam obrane računalne mreže koji uključuje odgovor na akcije i zaštitu kritične infrastrukture i zaštite informacija za organizacije, vladine entitete i druge moguće mreže. (Galinec i sur., 2017). Prepoznajemo ju kao dio koncepcijskog modela kibernetičke otpornosti i nalazi se u području sigurnosti informacijskog sustava (slika 2).



Slika 2: Kibernetička obrana u području sigurnosti informacijskog sustava informacijske sigurnosti

Kibernetički napad (eng. *Cyber Attack*) predstavlja čin ili radnju pokrenutu u kibernetičkom prostoru radi ometanja, poricanja, degradiranja ili uništavanja ugrožavanjem komunikacije, informacija i drugih elektroničkih sustava ili podataka koji se pohranjuju,

obrađuju ili prenose tim sustavima. Kibernetičke operacije su djelovanja u kibernetičkom prostoru (ofenzivne i defanzivne operacije) ili kroz njega (obavještajne i informacijske operacije) namijenjena očuvanju prijateljske slobode djelovanja u kibernetičkom prostoru i/ili stvaranju učinaka za postizanje zapovjednikovih ciljeva (NATO, 2020).

Kibernetičke operacije se sastoje od mnogih funkcija, procesa i aktivnosti koje obuhvaćaju kibernetičko upravljanje, kibernetički napad, kibernetičko iskorištavanje i kibernetičku obranu, uključujući aktivnosti. Po svojoj prirodi te su aktivnosti proaktivne, obrambene i regenerativne.

Nastavno, u kibernetičkom prostoru odvijaju se sljedeće vrste kibernetičkih operacija:

- **defanzivne** tj. obrambene kibernetičke operacije (eng. *Defensive Cyber Operations* - DCO) ,
- **ofanzivne** (eng. *Offensive Cyber Operations* - OCO),
- **obavještajne** (eng. *Cyber Intelligence, Surveillance and Reconnaissance* - CISR),
- **operativna priprema okružja** (eng. *Cyber Operational Preparation of the Environment* - COPE).

Nadalje, DCO sadržavaju aktivne i pasivne mjere za održanje sposobnosti uporabe kibernetičkog prostora te razlikujemo:

aktivnu obranu (eng. *Active Defence* - AD):

- aktivnosti koje ciljaju protivničke ofanzivne kibernetičke operacije kako bi se zadržala sloboda manevra (pokreta) unutar kibernetičkog prostora i

pasivnu obranu (eng. *Passive Defence* - PD):

- obrambene mjere sukladne vrsti ugroze s ciljem smanjenja učinkovitosti protivničkih kibernetičkih aktivnosti.

Aktivna kibernetička obrana kao podskup kibernetičke obrane usredotočuje se na integraciju i automatizaciju mnogih usluga i mehanizama za izvršavanje radnji odgovora u kibernetičkom vremenu. Sastoji se od skupa logičkih funkcija za prikupljanje detalja od arhitekture na razini poslovnog sustava do operativnog ostvarenja, prije svega s ciljem kako bi postala živi dio kibernetičkih operacija ministarstva obrane u obrani nacije od kibernetičkih protivnika.

Temeljna postavka oblikovanja novog koncepcijskog modela i razlikovanje informacijske sigurnosti, kibernetičke sigurnosti i kibernetičke otpornosti jest kriterij vrste kibernetičke ugroze/napada na informacijske sustave, s obilježjima rastuće složenosti, redoslijedom: CIA, APT, nulti dan (slika 1). Prema navedenom kriteriju, kibernetička sigurnost je širi pojam od informacijske sigurnosti jer obuhvaća složenije vrste napada nego što je to slučaj kod informacijske sigurnosti, u smislu poznavanja svojstava napada i odgovarajućih odgovora na njih (znanja o napadima i odgovorima na iste).

Dodatni kriterij za razlikovanje informacijske sigurnosti i kibernetičke sigurnosti je nepostojanje ili postojanje mrežne povezanosti sa vanjskim informacijskim sustavima (pr. putem interneta i/ili mreže utemeljene na bilo kojem mrežnom protokolu) poslovnog sustava (pr. korporacije). Podatkovna domena obje vrste sigurnosti kao i kibernetičke otpornosti je kibernetički prostor (sukladno definiciji danoj u poglavlju 2). U informacijskoj sigurnosti mrežna povezanost informacijskog sustava unutar poslovnog sustava može, ali i ne mora postojati (samostalna računala i drugi neumreženi uređaji s podatcima), dok se kod kibernetičke sigurnosti mrežna povezanost podrazumijeva.

Kibernetička sigurnost (slika 1) i kibernetička obrana (slika 2) nisu istoznačnice. Kibernetička obrana ponaša se dvojako u smislu pripadnosti informacijskoj ili kibernetičkoj sigurnosti; DCO su dio informacijske sigurnosti, dok OCO pripadaju kibernetičkoj sigurnosti. DCO (kibernetičku obranu prema kriteriju vrste operacija) razlikujemo kao pasivnu i aktivnu (opis u poglavlju 4.2). Dio su sigurnosti informacijskog sustava (slika 2) te time potpadaju pod informacijsku sigurnost - odnose se na informacijski sustav poslovnog sustava koji nije mrežno povezan s vanjskim sustavima. OCO nisu obuhvaćene oblikovanjem ovog modela te predstavljaju njegovo ograničenje, zbog zakonskog okvira. Po naravi su izvođenje operacija izvan granica informacijskog sustava poslovnog sustava kroz mrežnu povezanost s vanjskim sustavima te pripadaju kibernetičkoj sigurnosti. Kibernetička otpornost obuhvaća i informacijsku sigurnost i kibernetičku sigurnost.

Među brojnim potrebama borbenog osoblja, postoji potreba za sigurnošću, što uključuje koncepte ojačavanja, zaštite, napada i obrane među domenama borbenog osoblja kopnom, morem, zrakom, svemirom i kibernetičkim prostorom. Kibernetička sposobnost je integrirajuća za druge domene. Istodobno je i samostalna domena koja ima svoje jedinstvene potrebe za kibernetičkom obranom (Herring, Willett, 2014) .

Agilnost (okretnost) složenog sustava, kao sastavnica modela kibernetičke otpornosti, jedno je od svojstava potrebnih za izvršenje misije, a postiže se kroz obilježja proizvodnosti (djelotvornosti i učinkovitosti), fleksibilnosti, prilagodljivosti (adaptabilnosti) i svjesnosti (eng. *awareness*) sustava.

4.3 Razvoj i postizanje kibernetičke otpornosti

Kao što je prethodno spomenuto, kibernetička otpornost predstavlja sposobnost sustava,

organizacije, misije ili poslovnog procesa predvidjeti kibernetički napad, izdržati ga, oporaviti se te prilagoditi svoje sposobnosti u slučaju nepovoljnih uvjeta, stresova ili napada na kibernetičke resurse koji trebaju redovno funkcionirati.

Uspješnom provedbom mjera i postupaka kibernetičke sigurnosti i kibernetičke obrane rezultirat će učinkovitim (eng. *effective*) postupkom upravljanja rizikom tj. smanjenjem razine rizika koji se mora prihvatiti budući da se unutar informacijskog i komunikacijskog sustava ne može otkloniti, povećava se kibernetička otpornost.

Međutim, izazovi upravljanja rizikom u korelaciji su sa složenošću razvijenih sustava, s ranjivim komponentama, protokolima te sofisticiranošću vještina napadača.

U tu svrhu potrebno je otkrivati i prepoznavati ugroze (eng. *threats*) koje dolaze iz unutarnjeg i vanjskog okružja informacijskih i komunikacijskih sustava, te njihove ranjivosti (eng. *vulnerabilties*).

Tada je moguće iznalaziti načine i osiguravati sredstva poslovnih i razvojnih politika, ljudstva, materijala (tvari) i financija s ciljem (eng. *ends*) modeliranja i oblikovanja strategijskih procesa i izradu strategija za razvoj digitalnog društva, utemeljenog na načelima informacijske i kibernetičke sigurnosti.

Razvoj kibernetičke sigurnosti kao integralni dio razvoja digitalnog društva, razvoja osoblja, procesa, pravila (eng. *rules*) i tehnologija nužan je za izvedbu međusobno povezanih, cjelovitih poslovnih procesa „s kraja na kraj“ (eng. *End-to-End Processing* - E2E) organizacije.

Takva komunikacija i obrada odvija se unutar državnih tijela i drugih organizacija kao i međusobno, u svrhu isporuke sigurnih digitalnih usluga (eng. *Secure Digital Service*) u kibernetičkom prostoru od strane organizacija utemeljenih na ulogama (eng. *Role-Based Organizations*), vlasnika procesa (eng. *Process Owner*) i kibernetičkih timova za brzi odgovor i uzajamnu pomoć u kibernetičkoj sigurnosti (eng. *Cyber Rapid Response Team and Mutual Assistance* in Cybersecurity - CRRT & MA).

Za omogućavanje svega navedenog potrebno je ostvariti tehničku, semantičku, procesnu i pravnu interoperabilnost među subjektima razmjene podataka, informacija i znanja, uzimajući u obzir i primjenjujući načela kibernetičke sigurnosti i kibernetičke obrane na svim spomenutim razinama interoperabilnosti unutar arhitektura informacijskih i komunikacijskih sustava poticanih događajima (eng. *Event Driven Architecture* - EDA), arhitektura usmjerenih pružanju usluga (eng. *Service-Oriented Architecture* - SOA) ili neke njihove kombinacije (EDSOA), za razvoj digitalnog društva.

Scenariji kibernetičke obrane uvježbavaju se na kibernetičkom poligonu (eng. *Cyber Range* - CR, *Cyber Gym* - CG), softverskom alatu za uvježbavanje postrojbi za defanzivna i ofanzivna djelovanja na tehničkoj i taktičkoj razini u kibernetičkom prostoru. Alat i scenariji izgrađuju se suradnjom tijela državne uprave, akademske zajednice (istraživanje i razvoj sveučilišta u suradnji s državnim institucijama), gospodarstva (tvrtki) te međunarodnom obrambenom suradnjom. Time je moguće ostvariti višestruke pozitivne učinke po domaće gospodarstvo i razvoj digitalnog društva.

Sigurnosni operativni centar (eng. *Security Operational Center* - SOC) izrađuje se zbog povećanja razine sigurnosti informacijskih i komunikacijskih sustava te ostvarivanja odgovarajuće razine zaštite od naprednih prijetnji.

Uvođenjem u operativnu uporabu sve većeg broja sigurnosnih sustava i njihovom postupnom i konzistentnom integracijom povećava se potreba za pravodobnom vidljivosti, ispravnom prioritizacijom i eskalacijom, i gdje je god moguće, automatiziranim rješavanjem identificiranih sigurnosnih prijetnji.

U cilju odgovora na novonastale zahtjeve i ostvarenja sigurne obrade složenih poslovnih (sigurnosnih) događaja (eng. *Complex Events Processing* - CEP) ukazuje se potreba za uspostavom odgovarajućih procesa, pravila i tehnologija te posvećenog (eng. *dedicated*) dediciranog tima zaduženog za nadzor sigurnosti, sigurnosnih sustava i upravljanje sigurnosnim incidentima za uspostavom sigurnosno operativnog centara na razini organizacije. Sigurnosni operativni centar tako postaje temelj modernog i sigurnog informacijskog i komunikacijskog sustava.

5 Neki od novih rezultata istraživanja digitalne transformacije i sigurnosti

5.1 Preuzimanje računa

U f5 (2022) navodi se kako je preuzimanje računa (eng. *Account Takeover* - ATO) i dalje najrašireniji i najskuplji napad usmjeren na financijske institucije, tvrtke e-trgovine i mnoge druge organizacije. Nakon što je račun ugrožen, prevarant može isprazniti bankovne račune, odnosno, podići sredstva, kupiti robu ili usluge, pristupiti podatcima o plaćanju za korištenje na drugim stranicama, ili sudjelovati u nekim drugim zlonamjernim aktivnostima. Prema strategiji i istraživanju Javelin u njihovoj Studiji prijevare identiteta 2021., prijevara ATO dovela je do preko 6 milijardi dolara ukupnih gubitaka u 2020. (f5, 2022).

ATO često počinje napadima vođenim bot-ovima kao što je punjenje vjerodajnica - u kojima se prethodno ukradene vjerodajnice korisnika (eng. *credentials*) - korisničko ime i zaporka - i osobni identifikacijski podatci (eng. *Personal Identification Information* - PII) - ime, adresa, telefonski broj - koriste

za automatiziranu prijavu na korisničke račune. Mnogi od tih napada mogu se blokirati tradicijskim sigurnosnim rješenjima poput vatrozida (eng. *firewall*) aplikacija web-a utemeljenih na pravilima. No, sofisticirani prevaranti podižu razinu svog automatiziranog oponašanja ljudskog ponašanja, kako bi zaobišli kibernetičku obranu. Ako su dovoljno motivirani, napadači se ručno prijavljuju na račune, učinkovito zaobilazeći rješenja protiv automatizacije te provodeći prijevarne aktivnosti koje mogu dovesti do značajnih gubitaka.

I timovi za sigurnost i prijevare imaju vlastite alate za njihovo praćenje i otkrivanje, koji ciljaju specifične aspekte lanca vrijednosti prijevare i mogu pomoći u zaustavljanju prijevara. Izazov je što nema preklapanja odgovornosti ili dijeljenja podataka među tim timovima. Timovi za provedbu sigurnosnih operacija prate i reagiraju na sigurnosna upozorenja i automatiziraju i organiziraju sigurnosne mjere.

Analitičari prijevara usredotočuju se na reakciju na incident - pr. istragu osumnjičenih za prijevaru pri plaćanjima - i prilagođavaju pravila provjere autentičnosti na temelju lažno pozitivnih i lažno negativnih incidenata.

Prevaranti ciljaju na slaba mjesta u organizaciji silosima timova za kibernetičku obranu. Isti mogu, primjerice, ne uočiti incidente koji signaliziraju potencijalne prijevare prije nego što se one dogode, kao što je automatski napad punjenjem vjerodajnica koji vodi do ATO-a. Kao rezultat toga, timovi za prijevare troše nepotrebno vrijeme na reaktivnu analizu i napore za ublažavanje posljedica, što se moglo izbjeći dijeljenjem obavještajnih podataka između timova kibernetičke obrane.

Nasuprot tome, timovi mogu surađivati kako bi zaustavili napad na način koji ne utječe na rad korisnika. Zaustavljanjem automatiziranih napada, timovi za prijevare mogu se učinkovitije usredotočiti na ljudske/ručne aktivnosti prevaranta na sve točke lanca prijevare (eng. *Kill Chain*). To rezultira dramatičnim poboljšanjima u otkrivanju prijevara i prevencije, smanjenim gubitcima od prijevare i operativnim troškovima te ograničavaju (ako postoji) smetnju korisnicima u njihovu radu.

5.2 Izvješće o stanju strategije sigurnosti aplikacije

Prema jednom od novih istraživanja (f5, 2022) gotovo je 1500 donositelja odluka IT-a iz organizacija širom svijeta odgovorilo na osmo godišnje istraživanje o trenutačnom stanju primjene strategija. Podatci su prikupljani u razdoblju od tri tjedna u rujna i listopadu 2021.

Ovogodišnji rezultati uključuju prioritete iz širokog raspona industrija, s pružateljima usluga u oblaku, proizvodnja i obrazovanje zastupljeniji su nego u prošlosti. Tehnologija, financijske usluge i maloprodaja, distribucija ili tvrtke za profesionalne usluge također su bile dobro zastupljene. Sudjelovali su pojedinci iz organizacija svih veličina, dajući uvid u njihove trenutačne aktivnosti IT-a i izazove kao i njihova očekivanja za narednih nekoliko godina. Dok rezultati odražavaju nekoliko zanimljivih varijacija između regija ili industrija, općenito oni pružaju pouzdanu snimku perspektiva, potreba i smjera tipične organizacije IT-a danas. Rezultati također osvjetljavaju šire trendove i potencijalne zamke, kako poduzeća i institucije postaju sve više digitalna.

Organizacije rješavaju složenost pomoću umjetne inteligencije (eng. *Artificial Intelligence* - AI) i rješenja za inženjering pouzdanosti web-mjesta (eng. *Site Reliability Engineering* - SRE), dok uravnotežuju modernizaciju sa sigurnošću i vraćanjem aplikacija iz oblaka.

Ovogodišnje izvješće o strategiji stanja primjene pokazuje izazove s kojima se organizacije susreću dok transformiraju IT infrastrukturu za isporuku i sigurnost digitalnih usluga.

Rezultati istraživanja pokazuju kako se donositelji odluka iz područja IT-a još uvijek suočavaju s ograničenjima u svezi s modernizacijom, poslovnim imperativima i metodama implementacije dok ubiru prednosti digitalne transformacije. Organizacije se suočavaju s kontinuiranim traženjem ravnoteže između kontrola, troškova, korisničkog iskustva i zaštite aplikacija i aplikacijskih programskih sučelja (eng. *Application Programming Interface* - API).

Glavni nalazi uključuju:

- modernizacija se širi na manje vidljive poslovne procese i funkcije „stražnjeg ureda“ (eng. *Back-Office*),
- informacijski sustavi usmjereni na podatke i sustavi operativne tehnologije konvergiraju,
- gotovo svi ispitanici navode da im nedostaju kritični uvidi iz postojećih sustava,
- složenost postaje neodrživa, ometa performanse i degradira korisničko iskustvo,
- sigurnost se razvija u **upravljanje rizicima** jer je učinak i dalje najvažniji,
- repatrijacija je u porastu, premještajući aplikacije natrag u podatkovni centar iz oblaka.

U smislu razvoja sigurnosti, ovogodišnji rezultati istraživanja otkrivaju dobre vijesti, počevši od najbliže usklađenosti koju smo vidjeli između uloga čelnika IT-a i čelnika poslovanja o važnosti zaštite ne samo cjelokupnog poslovanja nego, također, infrastrukture i aplikacija.

Ovo teško stečeno poravnanje, potaknuto ugrozama i značajnim gubicima od prijevara, odražava konvergenciju poslovanja i ciljeva IT-a kako digitalna poduzeća sazrijevaju. Kako se složenost povećavala**,** nešto više viših čelnika IT-a ocijenilo je sigurnost -

osobito sigurnost aplikacije - puno važnijom nego što je to ocijenilo viših poslovnih čelnika. Ali, samo nekoliko postotnih bodova zajedničko je velikoj većini čelnika u obje uloge, kojima je takva zaštita prioritet.

Ipak, učinak je bitan, a više od tri četvrtine ispitanika su izjavili kako bi, ako bi mogli birati, isključili sigurnosne mjere u svrhu poboljšanja performansi. Polovica bi to učinila čak i za poboljšanja izvedbe manja od 50%. Ovo prilično šokantno preferiranje izvedbe uvijek je bilo istinito i djelomično može biti vođeno zahtjevima za sigurnosnom usklađenošću sustava, koji više izgledaju kao formalne mjerodavnosti nego učinkovita zaštita.

Ali, težnja za performansama u odnosu na sigurnost također odražava rast svijesti kako neosporivo ublažavanje prijetnji ne postoji. Ili, ako postoji, to bi uzrokovalo veće operativne troškove, frustracije korisnika ili gubitak prilike za poslovanje. Umjesto toga, sigurno digitalno poslovanje zahtijeva upravljanje spektrom rizika u svjetlu drugih ciljeva u stvarnom svijetu. To znači balansiranje prihvatljive izvedbe, korisničkog zadovoljstva i cijene uz prihvatljivu zaštitu i sigurnost.

Proaktivnost i kontekstualna inteligencija ključ su ove ravnoteže. Uvijek će biti važno brzo otkriti i neutralizirati značajnu sigurnosnu prijetnju, prije nego što ista prouzroči štetu. Zrelo upravljanje rizikom treba zanemariti reaktivna (a ponekad i proizvoljna) sigurnosna pravila, kao što su maksimalna duljina sesije. U takvom slučaju veća je vjerojatnost ugroze korisnika od bot-ova. Isti mogu potaknuti zlonamjernu automatizaciju, koja iskorištava nedostatke u tehnologiji i organizaciji kako bi se ugrozilo aplikacije, preuzelo korisničke račune i počinilo prijevaru. Stoga je ključno spriječiti automatizirane i ručne napade. Raščlamba ponašanja može dati rezultate takve inteligencije, a zrela organizacija može procijeniti rizik u kontekstu pružanja prilagodljive sigurnosti i performansi. Zrela digitalna sigurnost postaje još jedna domena cjelokupnog upravljanja rizicima poslovanja, posebice za digitalno napredna poduzeća.

Sigurnost je postala značajan trend. Trend je dijelom i odgovor na eksploziju mikroservisa (eng. *microservice*) koji se spajaju u redove „korisnika" čijem identitetu je potrebna provjera, čak i ako ta radna opterećenja komuniciraju samo unutar jednog podatkovnog centra. Osim toga, organizacije sa značajnim ulaganjima u API-je - uključujući one koji slobodno rabe „bilo što kao uslugu" (eng. *Anything as a Service* - XaaS) - trebaju modernizirati svoj pristup sigurnosti API-ja, a 78% ih je već implementiralo API sigurnosne mjere ili planiraju u sljedećih dvanaest mjeseci. Taj je omjer čak i veći, 91%, ako se uzmu u obzir i one- organizacije koje se nalaze na rubovima distribucije vjerojatnosti ovog istraživanja.

Sigurnost API-ja također sazrijeva, s organizacijama koje rabe različite pristupa, a mogu se grupirati u tradicijske, moderne i prilagodljive:

- manje od polovice ispitanika reklo je da cijene tradicijske metode, uključujući kriptiranje i dekriptiranje, provedbu ograničenja brzine, provedbu postupaka za smanjivanje najkritičnijih sigurnosnih rizika za web aplikacije (OWASP Top Ten), koje je spomenulo 45%, 33%, odnosno 30% ispitanika.
- suvremeni pristup autentifikaciji i autorizaciji korisnika (AuthN/AuthZ) 68% ispitanika smatra vrijednim, dok 58% cijeni još jedan moderan pristup, inspekciju prometa.
- konačno, 59% ispitanika je reklo da cijeni uporabu raščlambi ponašanja, kako bi se utvrdio legitimitet korisnika.

Sigurnost API-ja također je čimbenik u tehnologijama u sljedećih nekoliko godina. Konvergencija IT-a i OT-a te agilnost i poslovna učinkovitost koju ona obećava, zauzela je prvo mjesto. U težnji za većim performansama, „mreža pete generacije" (eng. *Fifth Generation Network* - 5G) dolazi na drugo mjesto, dijelom i zato što omogućuje veću uporabu „rubnog računarstva" (eng. *Edge Computing* - EC) i mogućnost povezivanja interneta stvari (eng. *Internet of Things* - IoT).

U kontekstu smanjenja rizika, danas je bitna sigurnost usmjerena na API - sigurnosni model s nultim povjerenjem (eng. *The Zero-Trust Security Model*) i web zaštita aplikacija i API-ja (eng. *Web Application and API Protection* - WAAP).

U jeku bolesti Covid-19, a i u sklopu pokušaja smanjenja složenosti, devet od 10 organizacija aktivno prilagođava svoje sigurnosne stavove, podiže svijest kroz obuku te istražuje dodatna rješenja i pristupe. Primjerice, u prošloj godini u 48% poduzeća povećano je usredotočenje na upravljanje ranjivostima i automatizaciju. Ostale ključne taktike uključuju usvajanje sigurnosti u oblaku, dodatnu obuku zaposlenika i konsolidacija dobavljača sigurnosti. U danima koji dolaze, većina organizacija morat će primijeniti nekoliko od ovih taktika u kombinaciji kako bi u dovoljnoj mjeri upravljale rizikom od narušavanja sigurnosti.

5.3 Daljnje istraživanje

Izradom koncepcijskog modela ostvaruju se pretpostavke za određivanje svih klasa i objekata (atributa, metoda i stanja), obilježja i procesa složenog sustava koji su važni za uspješno djelovanje konkretnog sustava u svrhu postizanja kibernetičke otpornosti, te postupnu evoluciju izrađenog modela u logički i fizički podatkovni model.

Prijedlog nove Direktive o sigurnosti mrežnih i informacijskih sustava 2 („Direktiva NIS2") u članku 5

koji se odnosi na nacionalnu strategiju kibernetičke sigurnosti traži da Strategija države članice EU posebno obuhvati:
- ciljeve i prioritete kibernetičke sigurnosti;
- konzistentne okvire upravljanja u područjima kibernetičke sigurnosti (kibernetičke krize, dijeljenje informacija, izobrazba) i po razinama (tehnička, operativna, strategijsko-politička), s ciljem postizanja željenih ciljeva i prioriteta, uključujući politike i odgovornosti različitih tijela i aktera uključenih u provedbu strategije;
- smjernice za utvrđivanje relevantne imovine i rizika kibernetičke sigurnosti;
- utvrđivanje mjera koje osiguravaju pripravnost, reakciju i oporavak od incidenata, uključujući suradnju između javnog i privatnog sektora;
- okvir politike za poboljšanu koordinaciju između mjerodavnih tijela prema Direktivni NIS2 i Direktivni o otpornosti kritičnih subjekata (koja se treba donijeti) u svrhu dijeljenja informacija o kibernetičkim prijetnjama, rizicima kibernetičke sigurnosti i incidentima, kao i na ne-kibernetičke prijetnje, rizike i incidente te izvršavanje nadzornih zadaća, prema potrebi;
- okvir politike za koordinaciju i suradnju između mjerodavnih tijela prema Direktivni NIS i mjerodavnih tijela imenovanih u skladu sa sektorskim zakonodavstvom.

Kao dio nacionalne strategije kibernetičke sigurnosti, države članice EU posebno trebaju usvojiti određene politike. Operativne politike (lanac opskrbe za proizvode IKT-a) moraju se provesti legislativno (transpozicijom Direktive NIS2). Strategijske politike (promicanja i razvoja obrazovanja i osposobljavanja) moraju se provoditi kroz strategiju i akcijski plan. To su politike:
- koje se bave kibernetičkom sigurnošću u lancu opskrbe za proizvode IKT-a i usluge koje rabe subjekti za pružanje svojih usluga,
- u svezi s uključivanjem i specifikacijom zahtjeva u svezi s kibernetičkom sigurnošću za proizvode IKT-a i usluge u javnoj nabavi, uključujući i kibernetičku sigurnosnu certifikaciju,
- upravljanja ranjivostima, koja obuhvaća primicanje i olakšavanje dragovoljnog koordiniranog otkrivanja ranjivosti,
- koje se odnose na održavanje opće dostupnosti, integriteta i povjerljivosti (CIA) javne jezgre otvorenog interneta,
- promicanja i razvoja obrazovanja i osposobljavanja za kibernetičku sigurnost, vještina, podizanja svijesti i inicijativa za istraživanje i razvoj,
- potpore akademskim i istraživačkim institucijama u razvoju alata za kibernetičku sigurnost i mrežne infrastrukture,
- relevantnih postupaka i odgovarajućih alata za dijeljenje informacija za potporu dragovoljnoj razmjeni informacija o kibernetičkoj sigurnosti između tvrtki, u skladu s pravom EU,
- koje se bave posebnim potrebama malih i srednjih poduzeća, osobito onih koji su isključeni iz područja primjene Direktive NIS2, u svezi s uputama i potporom u poboljšanju njihove otpornosti na kibernetičke prijetnje.

U svrhu izrade Direktive NIS2, za potrebe procjene učinka provedena je evaluacija funkcioniranja Direktive NIS, te su identificirani sljedeći izazovi (European Commission, 2020): niska razina kibernetičke otpornosti poslovnih sustava koji posluju u EU-u, nedosljedna otpornost u državama članicama i njihovim sektorima te niska razina zajedničke situacijske svijesti i nedostatak zajedničkog odgovora na krizu.

Buduća istraživanja evaluacije koncepcijskog modela kibernetičke otpornosti bit će provedena na način provjere sukladnosti njegovih sastavnica s definicijama te sadržajem istovrsnih pojmova buduće „Direktive NIS2“, nove Nacionalne strategije kibernetičke sigurnosti RH i novog Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti, čija je izrada u tijeku. Pri izradi navedenih strategijskih dokumenta, vođenoj od strane Nacionalnog Vijeća za kibernetičku sigurnost Vlade RH, primjenjuju se smjernice i privremene mjere (Europsko Vijeće, 2022) iz postojećeg prijedloga „Direktive NIS2“, stoga je potrebno osigurati snažnije upravljanje rizicima i incidentima, suradnju u tom području, te proširiti područje primjene pravila. Po usvajanju i donošenju istih, s obzirom na njihov sadržaj, u okviru budućih istraživanja potrebno je izraditi nove evaluacijske kriterije i izvršiti evaluaciju koncepcijskog modela.

6 Zaključak

Akteri kibernetičkih prijetnji, ugroza i napada današnjice jako se razlikuju po motivaciji, sofisticiranosti, razini resursa s kojima raspolažu i dubini specijalizacije. Istodobno, aplikacije postaju sve više distribuirane i decentralizirane, stvarajući potpuno novi svijet izazova i šteta. Kibernetička sigurnost predstavlja napor i djelovanje kao igru u kojoj nijedna organizacija ne može pobijediti u potpunosti. Ostati u toj igri moguće je samo uz dugoročnu strategiju, upornost i stalne inovacije.

Brza modernizacija, u uvjetima konvergencije sigurnosti IT-a i OT-a, nastavlja se u svim društvima diljem svijeta kako bi se postigao uspjeh, uključujući cjelovito, povjerljivo, raspoloživo (dostupno) i pouzdano digitalno iskustvo tj. robusnu zaštitu podataka i poslovanja. Kontinuirani napredak obuhvaća pristup sigurnosti koji se više temelji na obavještajnim podatcima i upravljanju rizicima. Zadržavanje trenutačnog zamaha digitalne

transformacije zahtijeva promjene u područjima ljudstva, procesa i tehnologije:

- rješavanje nedostataka u vještinama i izgradnja stručnosti u umjetnoj inteligenciji, strojnom učenju, upravljanju podatcima, usklađenosti i stvaranju sposobnijih timova za brzi odgovor;
- poboljšanje procesa, što uključuju šire usvajanje prakse SRE, kako bi se povećala operativna učinkovitost IT-a;
- konsolidacija telemetrije i skupova alata za upravljanje za sveobuhvatnom vidljivošću i nadzorom, uz dodatnu sigurnost i isporuku aplikacija tehnologije za rad u različitim okružjima.

Odgovaranjem na sva tri izazova, odjeli IT-a mogu svladati složenost višeslojnih arhitektura informacijskih sustava i distribuiranih aplikacija kako bi stekli vidljivost E2E, uz postizanje zaštite informacija, kibernetičke otpornosti kibernetičke i informacijske sigurnosti i kibernetičke obrane.

Ovim radom daje se uvid u načine, procese i sredstva za postizanje kibernetičke sigurnosti u današnjim uvjetima rastućih sigurnosnih prijetnji i najnovijih trendova digitalne transformacije, koja ih obuhvaća. U kontekstu kibernetičke otpornosti, predstavljen je novi koncepcijski model kibernetičke otpornosti koji obuhvaća kibernetičku sigurnost, informacijsku sigurnost i, unutar nje, sigurnost informacijskih sustava i kibernetičku obranu. Daljnja istraživanja, sukladno Direktivi NIS2 i EU usmjerena su prema pronalasku i uporabi učinkovitih procesa za agilnu (prilagodljivu, svjesnu, fleksibilnu i produktivnu) kibernetičku otpornost informacijskog sustava i atribuciju, planiranjem, razvojem i implementacijom opreme kibernetičkih sposobnosti te izobrazbe, obuke i osposobljavanja ljudstva. Cilj je postići stanje u kojem se sustav može uspješno suočiti s nepredvidljivim događajima (nepoznate nepoznanice). Navedeno se odnosi kako na unutarnje, tako i na njegovo vanjsko okružje. Isto se postiže kontinuiranom i dosljednom provedbom opisanih postupaka i procesa E2E te, posljedično, smanjenjem razine prihvatljivog rizika - svođenjem nepoznatih nepoznanica najprije na poznate nepoznanice te slijedno na poznate poznanice sustava koji radi u stvarnom vremenu. Tijekom istraživanja primijenjena je metoda koncepcijskog modeliranja s pripadajućim postupcima te je stvoren novi model kibernetičke otpornosti složenog sustava u kibernetičkom prostoru.

Kao znanstveni doprinos, ovim radom razvija se i unapređuje teorijska perspektiva kibernetičke otpornosti. Radom se sintetizira postojeće znanje i predstavlja ga se u novom kontekstu, kako bi se potaknulo razmišljanje i razvila situacijska svijest te se predlaže novi model za primjenu.

Literatura

European Commission (2020). Shaping Europe's digital future. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/nis-directive.

Europski parlament(2013). *Usvojeni tekstovi - Strategija za kibernetičku sigurnost u EU-u: otvoren i siguran kibernetički prostor.* Dohvaćeno s https://europarl.europa.eu/doceo/document/ TA-7-2013-0376_HR.html.

Europsko Vijeće (2022). Kibersigurnost: kako se EU bori protiv kiberprijetnji. Dohvaćeno s https://www.consilium.europa.eu/hr/policies/cybersecurity/

f5 (2022). *Overview.* 2022 State of Application Strategy Report.

Galinec, D., Možnik, D., Guberina, B. (2017). Cybersecurity and Cyber Defence: National Level Strategic Approach. *Automatika Journal for Control, Measurement, Electronics, Computing and Communications*, Vol. 8 No. 3, ISSN: 0005-1144, Taylor & Francis, London UK, pp. 266-272, 2017. doi:10.1080/00051144.2017.1407022.

Galinec, D., Steingartner, W. (2017). Combining Cybersecurity and Cyber Defense to Achieve Cyber Resilience. *IEEE 14th International Scientific Conference on Informatics - INFORMATICS 2017 (*pp. 87-93, 2017.). Institute of Electrical and Electronics Engineers, Inc., Poprad Slovakia.

Herring, M.J, Willett, K.D. (2014). Active cyber defense: a vision for real-time cyber defense. *J Inform Warfare*. 13(2):46- 55.

Hrvatski sabor (2007). *Zakon o informacijskoj sigurnosti*, Narodne novine 79/07.

Hrvatski sabor (2018). *Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga*. Narodne novine 64/18.

Hrvatski sabor (2021a). *e-doc - Hrvatski sabor*. Dohvaćeno s https://edoc.sabor.hr/.

Hrvatski sabor (2021b). Hrvatski sabor. Dohvaćeno s https://sabor.hr/.

NATO (2020). *Allied Joint Doctrine for Cyberspace Operations (AJP 3.20).* Edition A Version 1. NATO Standardization Office (NSO).

NATO Cyber Cooperative Cyber Defence Center of Excellence (2017). *Cyber Definitions*. Retrieved from https://ccdcoe.org/cyber-definitions.html.

Središnji državni ured za razvoj digitalnog društva (2021). *E-savjetovanja*. Dohvaćeno s https://esavjetovanja.gov.hr/ECon/Dashboard.

Središnji državni ured za razvoj digitalnog društva (2022). *Kibernetička sigurnost*. Dohvaćeno s https://rdd.gov.hr/izdvojeno/kiberneticka-sigurnost-1436/1436?big=1.

Vlada Republike Hrvatske (2015). *Nacionalna strategija kibernetičke sigurnosti*. Narodne novine 108/15.

Techopedia (2019). *Cyber Defense*. Retrieved from https://www.techopedia.com/definition/6705/cyberdefense.

United States Department of Defense (2011). *Strategy for Operating in Cyberspace*.

Zak, D. (2021). '*Nothing ever ends': Sorting through Rumsfeld's knowns and unknowns*. Retrieved from https://www.washingtonpost.com/lifestyle/style/rumsfeld-dead-words-known-unknowns/2021/07/01/831175c2-d9df-11eb-bb9e-70fda8c37057_story.html.

Cyber Security and Defense Insights: Designing a Conceptual Model of Cyber Resilience

Abstract

The planning of cyber security within a complex system and the application of its principles and procedures aims to achieve the system's resilience in cyber space, i.e. Cyber Resilience. The purpose of a complex system is to carry out a mission as a set of abilities and preferences with regard to the internal and external circumstances of the system. Achieving cyber resilience requires organizational, human, material and financial means in the implementation of measures, activities and procedures to reduce the level of residual (remaining) security risk. This is the part of the security risk that must be accepted within the system, since at the time of risk assessment with regard to internal and external circumstances as an opportunity to develop capabilities, it is not possible to achieve its further reduction. The conceptual research presented in this paper analyzes the ways and means for achieving cyber resilience in the conditions of today's growing security risks. The goal of this research is to create a new model of cyber resilience, which includes cyber and information security. The context of the model consists of unrecognized security risks in cyberspace, and the conceptual modeling method is used to design the model. The model implies and encompasses the awareness of the existence of unknown system vulnerabilities and at the same time unknown cyber threats and attacks as possible consequences of the existence of unrecognized vulnerabilities. This also takes into account the fact that the methods of preventing unprecedented threats Zero-Day Attacks in a large number of business cases are unknown today, as well as the methods of defense and possible responses to them - Unknown Unknowns. To confront the aforementioned challenges, there is a need to create "knowledge about ignorance" of a complex system, i.e. to develop cyber capabilities and their realization, based on the principles of cyber security and cyber defense.

Keywords: *attribution ; cyber attack ; cyber defense ; cyber resilience ; cybersecurity.*