Strateški plan

2021-2026

Sadržaj

I O organizaciji

Fondacija „Mreža za sajber bezbednost“, prethodno neformalno poznata i kao ’Petnička grupa’, razvijala se paralelno sa procesom uspostavljanja normativnog okvira u informacionoj bezbednosti u Srbiji. Nakon nekoliko manjih aktivnosti sprovedenih tokom 2014. godine , uz podršku tri međunarodne organizacije - Misije OEBS-a u Srbiji, Diplo Fondacije i Ženevskog centra za upravljanje sektorom bezbednosti (DCAF)- sredinom 2015. godine održan je prvi koordinacioni sastanak na kojem su učestvovale ključne javni i privatni akteri u oblasti sajber bezbednosti. Vremenom se ova zajednica, kroz redovne sastanke, rastuće članstvo, i nekoliko faza, razvila u neformalnu, multi aktersku grupu, sastavljenu od svih ključnih aktera na nacionalnom nivou u oblasti sajber bezbednosti iz javnog i privatnog sektora, akademske zajednice i civilnog društva. Od samog početka, zajednica je bila usredsređena na jačanje saradnje javnog i privatnog sektora i podršku razvoju adekvatnih politika i strateških okvira u oblasti sajber bezbednosti u Republici Srbiji. Tokom godina, zajednica se redovno sastajala i razgovarala o tekućim dešavanjima, pitanjima, potencijalima i izazovima u oblasti sajber bezbednosti u Srbiji, od normativnog okvira koji je razvijan tokom 2015. i 2016. godine, preko nacionalnih strateških prioriteta i usvajanja nacionalne Strategije razvoja informacione bezbednosti, do potrebnih i mogućih načina i oblika saradnje u oblasti sajber bezbednosti.

Nakon konsultativnog procesa koji je trajao tokom 2019. i 2020.-e, postignut je koncenzus da je zajednica dala značajan doprinos unapređenju nacionalnog okvira za sajber bezbednost, i da je formalizacija zajednice u obliku fondacije najbolji način da se pozitivan uticaj zajednice u narednim godinama zadrži i dalje razvija.

Fondacija još uvek nema nijednog zaposlenog, radi potpuno na volonterskoj osnovi, nema nikakav osnovni budžet ili infrastrukturu, a ovaj plan treba da pomogne u definisanju pravaca daljeg razvoja Fondacije i održavanja i razvoja nacionalne zajednice koja je čini.

II Analiza konteksta

Ključnu snagu Mreže predstavljaju ljudi koji su učestvovali u radu neformalne “Petničke grupe”, čije je delanje i dovelo do formalizacije grupe. Mreža je nastala iz zajednice koju čine stručnjaci i ljudi koji se praktično bave sajber bezbednošću u Srbiji (i šire), a koji rade u preko 30 različitih institucija i organizacija, iz javnog, privatno, akademskog i nevladinog sektora. Ova raznolikost donosi Mreži raznolikost ekspertize i kolektivnu mogućnost da kompleksne probleme sajber bezbednosti sagledava iz različitih uglova. Činjenica da je Mreža sastavljena od stručnjaka prepoznatih kako u svojim organizacijama i sektorima, tako neretko i međunarodno, omogućava da njeno delovanje bude usmereno znanjima i saznanjima koja nisu lako dostupna, a poverenje koje se gradilo između članova godinama, osigurava da se u Mreži može razgovarati otvoreno i bez zadrški, a informacije deliti bez bojazni za njihovu zloupotrebu na bilo koji način.

Slabosti koje Mreža treba da prevaziđe kako bi ostvarila svoj puni potencijal je to što postoji nedovoljna distinkcija između ličnog i/ili članstva u ime organizacije, kao i niz problema koji proizilaze iz činjenice da se formalno Mreža gradi od nule: ne postoji nikakva infrastruktura Mreže (kancelarija, zaposleni), sama organizacija nema nikakve reference (u smislu prethodnih projekata), a u tim uslovima je teško definisati jasnu viziju razvoja i tu viziju sprovesti.

Šanse za razvoj Mreže se mogu naći u činjenici da ona uživa poverenje državnih organa (kako nadležnih za sajber bezbednost, tako i za bezbednost uopšte), da je prepoznata u nacrtu nacionalne strategije za razvoj informacionog društva i informacione bezbednosti, kao i da je sama tema sajber bezbednosti sve aktuelnija kako donatorima, tako i drugim nevladinim organizacijama.

Pretnje razvoju Mreže se ogledaju pre svega u mogućem "tihom odumiranju" organizacije usled nemogućnosti definisanja i pokretanja konkretnih aktivnosti, kao i mogućnosti da neke druge, etabliranije nevladine organizacije, sa infrastrukturom koju Mreža nema, postanu dominantnije u nacionalnim raspravama vezanim za sajber bezbednost.

PEST analiza

Sajber bezbednost se na nivou Srbije i Balkana vidi kao važna tema, ali ne i kao tema koja donosi političke poene, pa samim tim neće biti u direktnom fokusu ključnih političkih aktera. Ovo nije nužno loša stvar, jer bi u takvoj situaciji stručna zajednica mogla da ima više mogućnosti da utiče na strateške procese. Prethodno iskustvo je pokazalo de moguće zaobići "visoku politiku", i ukoliko postoji inertnost na tom nivou, usmeriti se na rad na konkretnim aktivnostima, na stručnom nivou.

Postoji dobar odnos javnog i privatnog sektora u oblasti sajber bezbednosti, i Mreža, u svom prethodnom neformalnom obliku, je nesumnjivo tome pomogla. Inicijativa za Mrežu dolazi iz neformalnog sektora, ali njeno delovanje se tiče dosta toga što bi država trebalo da radi, a što je definisano postojećim zakonskim, strateškim i institucionalnim okvirima. Ipak, deo javnih finansija koji se odvaja za sajber bezbednost ne ukazuje na ozbiljniji pristup temi, kao ni strateški pristup – iako tu igra ulogu i generalni kapacitet javnog sektora (stanje javnih finansija, modernizacija javne uprave, i tome slično). Međutim, Mreža je i treba da ostane komplement državnih kapaciteta, ne da na bilo koji način preuzima ulogu državnih organa.

Ne postoji dovoljan nivo društvene svesti o tome da i samo društvo gubi zbog bezbednosnih rizika i propusta. Postoji generalno nerazumevanje pitanja bezbednosti, privatnosti, digitalne pismenosti; naročito oko suprotstavljenosti privatnosti i bezbednosti. Sajber je široka društvena tema koja ne dotiče samo određenu grupu u društvu.

Ekonomski, ne vidi se jasna dobit od ulaganja u sajber bezbednost, a sajber se ne vidi ni kao potencijalna ekonomska šansa. Ne postoji procena gubitaka na državnom nivou koji su posledica sajber napada/incidenata. Mala i srednja preduzeća, koja čine najveći deo srpske ekonomije, su posebno osetljiva na sajber napade.

Sajber bezbednost je tema koja je tu da ostane, koja u narednim godinama može samo da dobija na značaju. Razvoj novih tehnologija nosi nova rešenja za postojeće probleme, ali ii nove bezbednosne rizike. Bezbednost tehnologija će biti i pitanje javnih finansija, u smislu npr. nabavki velikih sistema za zaštitu kritične infrastrukture. Sa druge strane, bezbednost pojedinih tehnologija (5G, AI, i slično) postalo je i geopolitičko pitanje.

Nije izvesno da u zemlji postoji znanje da se isprati globalni tehnološki napredak. Sajber bezbednost je nedovoljno prisutan (ako uopšte) u istraživačkim projektima; u sistemu formalnog obrazovanja tek sporadično, ne sistemski, ne multidisciplinarno-uglavnom samo tehnički. Veliki problem je nepostojanje načina da se u istraživanja i obrazovanje vezano za sajber bezbednost uključe mladi: nema (ili nema dovoljno) labova, hakatona, malo je prilika za učenje i dokazivanje.

III Analiza ključnih aktera

Legitimitet Mreže crpimo iz pozicije da okupimo najbitnije aktere i znanja o sajber bezbednosti u Srbiji**.** Do sada je Mreža uspevala da okuplja aktere iz različitih sektora. Okosnicu okupljanja predstavljaju akteri iz javnog sektora, koji direktno kreiraju nacionalne politike. Međutim, Mreža je do sada uspevala da fasilitira otvoreni dijalog kreatora i nosioca javnih politika sa drugim relevantnim sektorima (privatni, akademski, NVO/stručni, čak i međunarodnim akterima), uvek na uzajamnu korist svih uključenih.

Državne/javne institucije su jako bitne i treba da ostanu bliske, ali treba napraviti i okvir za kontinuiranu saradnju i sa nedržavnim akterima (memorandumi o razumevanju treba da budu okvir za ovo, pre svih: MTTT, MUP-CERT, SHARE Fondacija, UBS, Unicom i SRB CERT/RATEL.

Jako je važno da se izbegne polarizacija zajednice kako se ona ne bi urušila**.**

Mapiranje i analiza ključnih aktera

Mape aktera (Anex) prikazuju kakva je situacija bila u prošlosti, ko su bili ključni akteri i kakav je bio njihov odnos prema Mreži i njenim aktivnostima. Ovo će se menjati u budućnosti, nije statična stvar. Uz to, i u zavisnosti od teme kojom Mreža bude odlučila da se bavi, imaćemo drugačije mape aktera, a samim tim i načine/nivoe angažovanja s njima.

Dobar način uključivanja različitih grupa aktera su i radne grupe: daju mogućnost fokusiranijeg rada na neku temu i angažovanja grupe aktera. Mreža treba da čim je pre moguću definiše početne radne grupe, donese odluku ko ih čini i šta je njihov mandat.

Aktere koji su važni, ali ne pokazuju preveliku zainteresovanost za učešće u radu Mreže treba uključiti kroz radne grupe, ili konkretne projekte/aktivnosti. Na duže staze, i kako se broj ovakvih sporazuma povećava, Memorandumi o saradnji takođe mogu biti opcija za definisanje i deklarisanje bliže saradnje.

IV Misija

Osnovni cilj Fondacije je unapređenje sajber bezbednosti u Srbiji uz aktivno učešće i saradnju državnih organa i institucija, privrede, akademskog sektora, organizacija civilnog društva i svih zainteresovanih aktera.

Misija Fondacije je da bude platforma za dijalog i saradnju različitih aktera i sektora koji su zainteresovani, stručni i udruženi u naporima da unaprede sajber bezbednost u Srbiji.

V Vizija

Mreža treba da bude prepoznata kao referentno mesto za dijalog i saradnju na temu sajber bezbednosti u Srbiji, kao akter koji kontinuirano i aktivno doprinosi kreiranju i sprovođenju jasne, inkluzivne, i efikasne nacionalne agende sajber bezbednosti.

Vizija Mreže je da u Srbiji:

- Sajber bezbednost postane „mejnstrim“ tema, tema koja se razmatra kao deo svih nacionalnih bezbednosnih i razvojnih politika u onolikoj meri u kojoj ostvarivanje tih politika zavisi od sajber-prostora i povezivanja ljudi i informacionih tehnologija u najširem smislu;
- Među-sektorska saradnja i dvosmerna komunikacija između države i nedržavnih aktera postane uobičajena, «prirodna» praksa, koja aktivno primenjuje kroz institucije i upravljačke prakse;
- Kapaciteti za sajber bezbednost budu dispergovani na sve relevantne aktere, uz jasne, jednoznačne linije odgovornosti za planiranje, odlučivanje i delovanje.

Sama Mreža doprinosi ovoj viziji kao ključni nacionalni resurs, zajednica koja je broker znanja između različitih aktera, priznat i prepoznat od svih relevantnih aktera.

VI Vrednosti

Principi i vrednosti na kojima organizacija temelji svoj rad i koje dele svi njeni članovi su sledeći:

- **Poverenje.** Članice veruju jedne drugima, uz prihvatanje njihovih individualnih karakteristika ukoliko se njihovi ciljevi i načini delovanja podudaraju sa misijom Mreže. U cilju utvrđivanja ove podudarnosti, mehanizmi i procedure za interno procenjivanje i odobravanje novih članova će biti uspostavljeni.
- **Otvoreni dijalog.** Neslaganja i različiti pogledi su dobrodošli, ali ne i konfliktna atmosfera.
- **Stručnost u temi.** Deo zajednice su pojedinci koji su predstavnici nadležnih institucija ili značajnih organizacija, ali i pojedinci iz zajednica praksi koji mogu da doprinesu ciljevima Mreže.
- **Nepristrasnost.** Mreža nema nadzornu („watch-dog“) ulogu, ali nije ni tzv. „državna organizacija civilnog društva“ („GONGO“). Njen cilj je da pomogne ostvarivanju javnog interesa kroz davanje predloga i komentara, i nepristrasnu, konstruktivnu kritiku. Mreža neće braniti strane u konfliktu, već ideje i procese koji doprinose opštem interesu - većem nivou sajber bezbednosti u Srbiji.
- **Saradnja.** Rad Mreže je baziran na principima multi-akterske saradnje i javno -privatnog partnerstva u cilju javnog dobra/interesa.

VII Strateški ciljevi (programski)

STRATEŠKI CILJ 1: Ojačati multi-akterski dijalog i uticaj na sajber politike i modele upravljanja (governance) uspostavljanjem efikasnih i održivih mehanizama i praksi

Od svojih neformalnih početaka 2014-2015. godine, pa do formalnog organizovanja i prelaska u novu fazu rada, cilj i razlog funkcionisanja Mreže bio je i ostao dijalog različitih nivoa društva u Republici Srbiji o najvažnijim pitanjima vezanim za sajber bezbednost; prevashodno komunikacija i razmena ideja predstavnika državnih institucija, privatnog sektora i akademske zajednice, odnosno organizacija civilnog društva. Imajući ovo u vidu, prvi strateški cilj Mreže je dalje jačanje već uspostavljenog dijaloga. Isti treba da se ostvaruje na više načina. U organizacionom smislu, pre svega kreiranjem mehanizama za uspostavljanje njegove održivosti, stalnosti, dalje fokusiranosti i poštovanja posebnih interesovanja pojedinih učesnika, odnosno formalizacijom saradnje Mreže sa sopstvenim „članstvom”. U kontekstualnom smislu, Mreža treba da nastavi da bude mesto susreta stručnjaka u ovoj oblasti, da produkuje kvalitetan materijal, da omogući kritički osvrt na zakonski i strateški okvir, odnosno na uspostavljene sisteme komunikacije različitih aktera. Konačno, cilj Mreže je i da prati dešavanja i omogući kreiranje partnerstava i na regionalnom, evropskom i globalnom

nivou, sa jedne strane usvajajući primere dobre prakse, ali i šireći svoj pozitivan primer van granica Republike Srbije.

Operativni cilj 1.1: Uspostavljanje kontinuiranog dijaloga o sajber bezbednosti na opštem (generalnom) nivou

Mere:

1.1.1. Definisanje formalnih sporazuma Mreže sa svim relevantnim (i zainteresovanim) akterima u Srbiji, u skladu sa definisanim ciljevima Mreže, a sa ciljem njene dalje legitimizacije i pozicioniranja u odnosu na svoje članstvo

1.1.2. Održavanje redovnih tematskih sastanaka Mreže, u zavisnosti od interesovanja učesnika Mreže za određene teme, trenutnih potreba i aktuelnosti tema

1.1.3. Organizacija konferencija, panela, okruglih stolova, debata, koji bi uključili i širu zajednicu, dalje popularizovali temu, ali i postavili Mrežu u poziciju organizacije koja je “etalon” za teme sajber bezbednosti u Srbiji.

1.1.4. Uspostavljanje radnih grupa unutar Mreže kako bi se omogućilo fokusirano delovanje i saradnja u skladu sa interesima i ekspertizom njenih članova

Operativni cilj 1.2: Sprovođenje stručnih analiza postojećih okvira i predloga politika - uključujući postojeće, kao i predloge novih zakona (i podzakonskih akata), strategija i planova

Mere:

1.2.1. Redovni godišnji sastanci/radionice vezane za unapređenje zakonodavnog i strateškog okvira, pregled implementacije strategije i drugih aktivnosti u zavisnosti od trenutnih dešavanja, trendova i inicijativa

1.2.2. Pravovremen analize zakonodavnog i strateskog okvira, kapaciteta, međunarodnih obaveza, itd. i kreiranje tzv. „shadow” izveštaja

1.2.3. Simulacije sajber incidenata kroz vežbe (multi-akterske „table-top” vežbe na nivou politika) na osnovu kojih se takođe daju predlozi za izmene i dopune postojećih okvira i mapira dobra praksa

1.2.4. Procena usklađenosti relevantnog (šireg) zakonodavstva i strateških dokumenata sa normativnim i strateškim okvirom informacione bezbednosti („mainstreaming“, uvođenje dimenzije sajber bezbednosti), razvoj vodiča i smernica i digitalnih alata za samoprocenu

Operativni cilj 1.3: Uspostavljanje međunarodne saradnje i razvojnih inicijativa-projektovanje međunarodne prepoznatljivosti u saradnji sa nacionalnim akterima, u cilju izgradnje „privlačnosti” Mreže i uspostavljanja saradnje sa međunarodnim partnerima na zajedničkim inicijativama, programima i projektima

Mere:

1.3.1. Kontinuirano mapiranje regionalnih i međunarodnih aktera i dešavanja u oblasti sajber bezbednosti u cilju identifikacije potencijalnih međunarodnih partnera i inicijativa koje bi Mreža podržala/u koje bi se uključila

1.3.2. Uspostavljanje komunikacije sa relevantnim regionalnim i međunarodnim organizacijama (npr. ITU, OSCE, RCC) i mrežama (npr. ECSO, Cyber Security

Coalition, i sl.) u cilju razmene iskustava i pozicioniranja Mreže na regionalnom/globalnom nivou

1.3.3 Uspostavljanje partnerstava sa relevantnim akterima u regionu (nadležnim ministarstvima, CERT-ovima, privatnim sektorom, organizacijama civilnog društva i/ili akademskim institucijama i istraživačkim centrima) u cilju promocije Mreže i njenog modela saradnje, razmene iskustava i daljeg povezivanja aktera iz javnog i privatnog sektora u regionu.

1.3.4 Organizacija studijskih poseta sličnim mrežama i inicijativama javno-privatnih partnerstava u inostranstvu, predstavljanje Mreže na regionalnim i međunarodnim događajima.

STRATEŠKI CILJ 2: Uticati na razvoj svesti šire javnosti o značaju sajber bezbednosti, odnosno na izgradnju poverenja u ključne nosioce ove teme, podizanjem informisanosti i znanja

Sajber bezbednost je tema koja dotiče (i doticaće) sve aspekte društva u savremeno doba. Zbog toga nije dovoljno razmatrati je samo na nivou stručne zajednice - potrebno je podizati svest o njenom značaju za različite nivoe organizovanja upravljanja, do nivoa ranjivih grupa i različitih društvenih uloga koje mi, kao pojedinci imamo u različitim fazama naših života. Mreža za sajber bezbednost, kao sveobuhvatna stručna zajednica ima jedinstven kapacitet da dopre do različitih društvenih grupa i ukaže na važnost odgovornog ponašanja u digitalnom svetu. Zbog toga je potrebno da se, sa jedne strane, radi ciljano sa različitim društvenim grupama (zaposleni u javnoj upravi, zaposleni u velikim korporacijama, vlasnici mikro, malih i srednjih preduzeća), ranjivim delovima stanovništva (deca, žene, stariji), ali i da se ostvari ‘sinergija’ različitih aktivnosti ovog tipa, bez želje da se one centralizuju, već da budu koordinisane i komplementarne.

Operativni cilj 2.1: Osnaživanje državnih i nedržavnih aktera kroz podizanje svesti i razvoj alata koji podržavaju uspostavljanje osnovnih praksi sajber bezbednosti

Mere:

2.1.1. Razvijati mrežu partnerstava sa relevantnim akterima iz privatnog sektora i civilnog društva na nacionalnom i lokalnom nivou sa ciljem rada na podizanju svesti

2.1.2. Razvoj programa i vodiča, kao i digitalnih alata (npr. alata za samoprocenu) o osnovama sajber bezbednosti i sajber higijene, prilagođenih različitim grupama državnih i nedržavnih aktera (npr. državna administracija generalno, lokalne samouprave, mala i srednja preduzeća, civilno društvo, mediji)

2.1.3. Kontinuirano mapiranje i (gde je moguće) koordinacija različitih inicijativa usmerenih na podizanje svesti i aktera koji ih sprovode, u cilju potencijalnog uspostavljanja partnerstava, uvezivanja inicijativa u veće kampanje, kao i razmene iskustava i dobrih praksi generalno (npr. kreiranje baze podataka o relevantnim aktivnim inicijativama i projektima)

Operativni cilj 2.2: Promovisanje sajber bezbednosti kao teme i neophodne prakse sajber higijene u široj javnosti, sa posebnim fokusom na ranjive grupe

Mere:

2.2.1. Uspostavljanje redovnog istraživanja javnog mnjenja o sajber pismenosti u društvu, sa ciljem analize trenutnog stanja, praćenja trendova, i mapiranja postojećih „slabih tačaka" na koje bi trebalo usmeriti pažnju, odnosno adekvatnog planiranja aktivnosti na osnovu „stanja na terenu"
2.2.2. Uspostavljanje saradnje sa medijima, posebno novinarima koji pokrivaju ovu i srodne teme, u cilju podrške boljoj informisanosti samih novinara o temama vezanim za sajber bezbednost pa tako i kvalitetnijeg sadržaja i bolje informisanosti šire javnosti; ali i potencijalno lakšeg plasiranja tema od važnosti za Mrežu
2.2.3. Razvoj programa i vodiča, u štampanom i digitalnom formatu (u zavisnosti od ciljne grupe) o osnovama sajber bezbednosti i sajber higijene i izvođenje radionica i predavanja prilagođenih konkretnim problemima i izazovima sa kojima se suočavaju različite ranjive grupe u društvu (npr. deca, žene, starije osobe)
2.2.4. Uspostavljanje partnerstava sa javnim institucijama na lokalu
2.2.5. Uspostavljanje redovne kampanje sa kontinuiranim aktivnostima - uključujući kreiranje informativnog materijala i diseminacija različitih sadržaja putem medija i društvenih mreža - u saradnji sa članicama Mreže, ali i širom zajednicom zainteresovanih aktera, kako bi se doprelo do što je većeg broja građana i građanki, a Mreža pozicionirala kao jedan od ključnih aktera i nosilac napora usmerenih na podizanje svesti u široj javnosti

STRATEŠKI CILJ 3: Povećati kapacitete članica Mreže i nacionalnih institucija zaduženih za sajber bezbednost za aktivno uključivanje u definisanje i sprovođenje jasnih, efikasnih i inkluzivnih politika sajber bezbednosti u Srbiji

Da bi Mreža ostvarila svoju viziju, neophodno je da konstantno radi na unapređenju kapaciteta svojih članica, ali i ostalih zainteresovanih aktera koji su donosioci odluka ili u poziciji da ostvaruju društveni uticaj u ovoj oblasti. Razvijanje Mreže kao prepoznatljivog mesta za razvoj kapaciteta doprineće održivosti angažmana postojećih aktera i članova, stimulisati potencijalno pasivne članove, ali i animirati nove. Mreža treba da se profiliše kao jedinstvena zajednička platforma za razvoj znanja, veština i praksi potrebnih za efikasno upravljanje sajber bezbednošću. Mreža će nuditi multidisciplinarne obuke i radionice, ne kao konkurencija formalnim obrazovnim programima i firmama koje pružaju IKT obuke, već kao njihov „suplement". Zato će pristup Mreže biti sledeći:

- **Izgradnja znanja** će se pre svega obavljati kroz aktivnosti „učenja od kolega (peer learning)", mentorstvo i slično;
- **Izgradnja veština** će se obavljati primarno kroz praktičan rad, bilo kroz zajedničke projekte članica (i ne-članica) ili vežbe/simulacije;
- **Izgradnja praksi** kojima se nadležnim institucijama nudi mogućnost nadomeštanja nedostajućih kapaciteta (znanja, ljudi, veština) kroz različite oblike saradnje sa nedržavnim akterima (pre svega, ali ne isključivo, kroz Mrežu)

Operativni cilj 3.1: Izgradnja kapaciteta članica Mreže

Mere:

3.1.1. Program obuka „u Mreži“

Razvoj programa obuka za članove mreže od članova mreže - po dogovorenom godišnjem planu, svako iz svoje oblasti, vezane za praktičan rad (npr. MTTT o procesu donošenja i sprovođenja zakona, UBS o sprečavanju finansijskog sajber kriminala, MUP o VTK). Obuke bi za članovima Mreže bile ponuđene bez nadoknade.

3.1.2. Mentorstva, učenje na radnom mestu

Uspostavljanje mentorskih i programa učenja na radnom mestu u članicama Mreže, gde bi sama Mreža bila „most“ između institucija i organizacija koje takve programe nude, koja nalazi i uvezuje zainteresovane strane na osnovu potrebe i ponude, i fasilitira samu razmenu kao garant poverenja

3.1.3. Senzibilizacija rukovodstva kroz podizanje svesti

Organizacija programa usmerenog na podizanje svesti/obuka za rukovodioce uz učešće predstavnika drugih sektora, u cilju boljeg razumevanja problematike, trendova i rizika u ovoj oblasti iz uglova gledanja različitih sektora, kao i podrške donosiocima odluka za razumevanje nacionalnog ekosistema sajber bezbednosti.

3.1.4. Radionice

Razvoj programa obuka, praktičnih radionica i „table-top” vežbi koji uključuje i učešće i/ili podršku eksternih partnera

Operativni cilj 3.2: Izgradnja kapaciteta ključnih sektora i aktera koji nisu deo Mreže

Mere:

3.2.1. Uparivanje potreba javnog sektora za efikasno upravljanje sajber bezbednošću sa mogućnostima doprinosa ne-državnih aktera

Uspostavljanje platformi za deljenje informacija (npr. pravljenje ISAC-a), koje bi bile komplementarne sa postojećim državnim, aktivno ohrabrivanje i fasilitiranje praktičnih oblika deljenja informacija i iskustava

3.2.2. Sprovođenje projekata i analiza potreba izgradnje kapaciteta za druge aktere

Na primer, za lokalne samouprave, mala i srednja preduzeća i sl. na nekomercijalnoj osnovi

3.2.3. Uspostavljanje saradnje sa obrazovnim institucijama

Uspostavljanje saradnje sa institucijama nadležnim za politike obrazovanja, u cilju razvoja zajedničkih inicijativa i programa usmerenih na razvoj tržišta radne snage u oblasti sajber bezbednosti u Srbiji

STRATEŠKI CILJ 4: Institucionalni razvoj Mreže i izgradnja operativnih kapaciteta radi ostvarivanja zadatih programskih i strateških ciljeva

Fondacija predstavlja nastavak rada neformalne mreže velikog broja relevantnih aktera koji deluju u oblasti sajber bezbednosti. Neformalnost je Mreži dala fleksibilnost učešća, omogućila da zajednica raste i bude prepoznata kao relevantan sagovornik od strane državnih organa, i kroz konsultativni proces tokom 2019/2020, svi su se složili da njeno postojanje treba formalizovati kao Fondaciju.

Fondacija sa druge strane još uvek nema jasnu organizacionu strukturu, održive finansijske i ljudske resurse, godišnji finansijski plan, ni plan za prikupljanje sredstava po planiranim programskim aktivnostima (Fundraising plan). Takođe, Fondacija nema svoje zvanične prostorije dok je web stranica u fazi izrade. Fondacija ima svoj Upravni odbor ali i Savetodavni odbor koji ima mogućnost da značajno utiče na rad Mreže, kao i da vrši kontrolnu funkciju u određenoj meri, posebno kada se radi o temama i oblastima kojima se Mreža bavi.

Ovaj strateški cilj treba da doprinese definisanju pravca daljeg organizacionog razvoja Mreže kako bi bila u stanju da efikasno odgovori na zahteve koji proističu iz postavljenih strateških i programskih ciljeva. S tim u vezi, razvoj organizacionih i ljudskih kapaciteta treba biti posvećen stvaranju održivih uslova za sprovođenje aktivnosti Mreže u pogledu:

a) facilitacije/koordinacije multi-akterskog dijaloga kroz nove mehanizme i prakse;
b) podizanja informisanosti, znanja i razvoja svesti šire javnosti o značaju sajber bezbednosti;
c) unapređenja kapaciteta članica mreže i nacionalnih institucija;
d) stvaranja baze znanja i ekspertize u oblasti sajber bezbednosti.

Operativni cilj 4.1: Uspostaviti organizaciono-upravljačke procese Fondacije

Mere:

4.1.1. Izrada unutrašnjih akata i regulative potrebne za redovno funkcionisanje Fondacije u skladu sa propisima

Priprema seta pravilnika i unutrašnje regulative u pogledu odnosa između upravljačkih struktura odnosno Upravnog Odbora i Savetodavnog Odbora i izvršnog dela Fondacije odnosno menadžmenta. Izrada i usvajanje plana rada UO, formulara za izveštavanje, pravilnika o radu, etičkih kodeksa, regulative vezane za pitanja odnosa među zaposlenima, medijacije, prevencije mobinga, diskriminacije, uznemiravanja i sl.

4.1.2. Priprema finansijskih i računovodstvenih procedura, pravilnika o korišćenju sredstava i resursa Fondacije

4.1.3. Uspostavljanje sistema vođenja i upravljanja kancelarijskim poslovanjem, zavođenja predmeta i zapisnika sa sastanaka

4.1.4. Definisanje modela izveštavanja o radu Fondacije, plan komunikacije ka Mreži, široj zajednici i javnosti

4.1.5. Uspostavljanje plana za prikupljanje donacija (Fundraising plan)

4.1.6. Izrada uputstva i formulara za objavljivanje sadržaja na web stranici Fondacije

Operativni cilj 4.2: Izgraditi kapacitete za upravljanje Mrežom, izgradnja i održavanje odnosa sa članstvom

Mere:

4.2.1. Angažovanje projektnog koordinatora i finansijskog koordinatora koji će se starati o redovnom funkcionisanju Fondacije

Kratkoročno, potrebno je pronaći i model angažovanja osoba koje bi za prvo vreme bile zaposlene na pola radnog vremena, dok se ne obezbede održivi izvori finansiranja.

4.2.2. Organizacija redovnih (dva puta godišnje) radionica namenjenih za članove Mreže u cilju definisanja projektnih ideja

4.2.3. Organizacija kvartalnih sastanaka Savetodavnog odbora i prezentacija kvartalnih izveštaja o radu Fondacije

4.2.4 Definisanje sistema i procedura za uključivanje članova Mreže u sprovođenje aktivnosti, obaveštavanje o aktivnostima, korišćenje ekspertize, promovisanje članova Mreže, izgradnju organizacione kulture zajednice

4.2.6. Mapiranje potencijalnih novih članova, pojedinaca i/ili institucija koji stručno i vrednosno odgovaraju ciljevima Fondacije

Operativni cilj 4.4: Ojačati operativno-tehničke kapacitete Fondacije

Mere:

4.4.1. Iznajmiti i opremiti prostor u skladu sa finansijskim planom

4.4.2. Angažovati knjigovodstvene usluge i pripremiti finansijske i računovodstvene dokumente

4.4.3. Obezbediti IKT uslove neophodne za svakodnevni rad i komunikaciju

4.4.4 Obezbediti pravne usluge u vezi radnih prava i regulative vezane za poslovanje Fondacije