SMJERNICE ZA STRATEŠKI OKVIR CYBER SIGURNOSTI U BOSNI I HERCEGOVINI

Sarajevo, oktobar 2019. godine

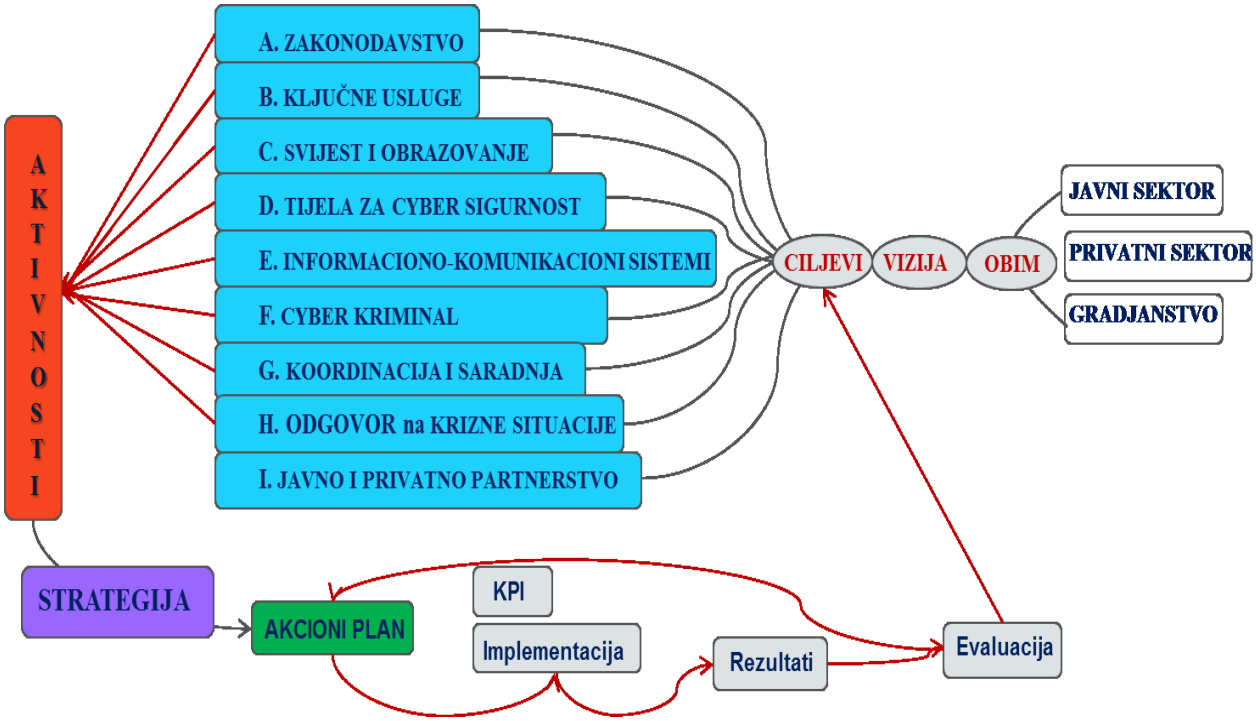
Organization for Security and Co-operation in Europe
Mission to Bosnia and Herzegovina

Misija OSCE-a u BiH je podržala izradu ovog dokumenta. Svako gledište, izjava ili mišljenje, izraženo u ovom dokumentu, a za koje nije izričito naznačeno da potiče iz Misije OSCE-a u BiH, ne odražava nužno zvaničnu politiku Misije OSCE-a u BiH.

Sadržaj

VIZIJA (5 godina)

Vizija Strateškog okvira za cyber sigurnost u Bosni i Hercegovini je da se, u skladu sa realnim potrebama, potencijalnim prijetnjama, kao i međunarodnim obavezama i standardima u oblasti cyber sigurnosti, te u skladu sa nadležnostima, osigura strateški i zakonski okvir, te unaprijede procedure i tehnike u cilju zaštite informaciono-komunikacionih sistema i krajnjih korisnika u cyber prostoru. Ostvarenjem vizije postiže se smanjenje rizika, uz uvažavanje privatnosti, te istovremeno promovišu tehničke inovacije, olakšava komunikacija, ekonomski razvoj i transparentnost, kao i sigurnost sveu kupnog društva.



Slika 1.

I. Smjernice za razumijevanje strateškog okvira

Savremeno društvo se u značajnoj mjeri oslanja na pogodnosti i inovacije koje nude informaciono-komunikacione tehnologije, a koje su postale nezaobilazni faktori u svim sferama života i djelovanja. Razvoj komunikacionih tehnologija dešava se velikom brzinom na globalnom nivou uvezivanjem ljudi i uređaja po cijeloj planeti u sveobuhvatni sistem koji zovemo Internet. Državne službe, kritična infrastruktura, uključujući finansijski sektor, energetski sektor, vojni i sigurnosni sektor, zatim bolnice, servisi, kompanije, škole i građani, sve više i nepovratno zavise od međusobne povezanosti i globalne mreže. Globalna uvezanost, razvoj tehnologije i digitalnog okruženja znači i da su efekti ovog razvoja sveobuhvatni - od pozitivnih i afirmativnih do onih rizičnih i negativnih efekata. Ugrožavanje sigurnosti cyber[1] prostora, bilo da se radi o cyber prijetnjama, terorizmu, eskalaciji odnosa među državama, nelegalnoj trgovini, svim vrstama cyber kriminala i zloupotreba, odavno nije u okvirima lokalnog ili državnog, nego međunarodnog. Cyber prostor sada se sve više prepoznaje kao nova oblast sukoba, te zemlje u svoje tradicionalne elemente uključuju cyber elemente vojne doktrine ili razvijanje ofanzivnih cyber sposobnosti i cyber vojnih komandi. Također se na globalnom planu ubrzano radi na međunarodnom zakonodavstvu koje bi garantovalo siguran, otvoren i stabilan cyber prostor.

Bosna i Hercegovina, kao članica međunarodnih organizacija, se obavezala na poštivanje obaveza, principa i standarda koji proizlaze iz članstva u ovim organizacijama, bilo da se radi o Ujedinjenim nacijama (UN-u), Organizaciji za sigurnost i saradnju u Evropi (OSCE-u), regionalnim inicijativama ili obavezama na putu pridruživanja Evropskoj uniji. Jedna od međunarodnih obaveza Bosne i Hercegovine je implementacija OSCE-ovih Mjera izgradnje povjerenja za smanjenje rizika od konflikta, koji proizlazi iz korištenja informacionih i komunikacijskih tehnologija, koje je usvojilo Stalno vijeće OSCE-a, kako bi se osigurao otvoren, interoperativan, siguran i pouzdan Internet u državama članicama OSCE-a, te smanjili rizici od pogrešne percepcije i mogućeg izbijanja političke i vojne tenzije ili sukoba. Strateški cilj Bosne i Hercegovine je priključenje EU kroz pristupne pregovore do punopravnog članstva. Jedan od elemenata koji treba ispuniti tokom ovog procesa je adekvatan nivo cyber sigurnosti. Direktiva (EU) 2016/1148 Evropskog parlamenta i Vijeća o mjerama za visoki zajednički nivo sigurnosti mrežnih i informacionih sistema širom Unije, poznatija kao NIS direktiva[2] (*EU Network and Information Security Directive*), između ostalog nalaže da svaka država članica donosi

[1] Termin „cyber“ (sajber; kibernetski / kibernetički prostor; eng. Cyber (space)) se koristi u ovom dokumentu i označava prostor koji je široko rasprostranjen i međupovezan digitalnim tehnologijama, uspostavljen uz pomoć i posredovanje kompjutersko-digitalne tehnologije. Pojam cyber prostor se danas koristi za sve što je na Internetu.

[2] NIS direktiva: (eng.) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
(hr.) DIREKTIVA (EU) 2016/1148 EUROPSKOG PARLAMENTA I VIJEĆA od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije
Dostupno na: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

svoju strategiju za sigurnost informaciono-komunikacionih sistema. Ratificiranjem Konvencije Vijeća Evrope o cyber kriminalu (Budimpeštanska konvencija) postoji potreba borbe protiv cyber kriminala i u okviru ovih međunarodnih obaveza[3]. Bosna i Hercegovina je potpisnik Pakta stabilnosti – inicijativa za elektronsku jugoistočnu Evropu – eSEE 2007. godine, kojom se afirmiše regionalna saradnja, te rast i razvoj elektronskih komunikacija. Nepoštivanje ovih obaveza i neučestvovanje u naporima za realizaciju zajedničkih mjera sigurnosti može imati nepovoljne posljedice za Bosnu i Hercegovinu, ne samo u kritičnom tehničkom domenu, nego i u diplomatskom i političkom smislu.

Broj uređaja povezanih na Internet raste eksponencijalno, kao i broj aktivnih korisnika Interneta[4], što ukazuje na pozitivan razvoj bosanskohercegovačkog društva. Cyber prostor nudi mnoge mogućnosti za rastuće ekonomije i građane i pomaže u zatvaranju jaza između bogatih i siromašnih. Postojeće, kao i razvojne kapacitete, neophodno je zaštititi, uzimajući u obzir izloženost i rastuće prijetnje u cyber prostoru.

Međutim, kao što je i navedeno u Izvještaju Evropske komisije o napretku Bosne i Hercegovine već davne 2016. godine: „Bosna i Hercegovina nema sveobuhvatni strateški pristup za rješavanje pitanja prijetnji u oblasti cyber kriminala i cyber sigurnosti.“ Navodi se da je potrebno ojačati reagovanje na prijetnje u oblasti cyber sigurnosti, postojeće kapacitete za borbu protiv cyber kriminala, kao i kapacitete timova za prevenciju i zaštitu od cyber incidenata i prijetnji sigurnosti javnih informacijskih sistema (CERT/ CSIRT)[5].

Postojeći ljudski i materijalni kapaciteti, te kapaciteti organizacija nisu dovoljni da osiguraju potreban nivo sigurnosti u cyber prostoru u Bosni i Hercegovini. Različiti nivoi vlasti imaju različite nivoe pripremljenosti, koji su doveli do različitog pristupa pitanjima cyber sigurnosti u okviru Bosne i Hercegovine. Rezultat je nejednak nivo zaštite korisnika, kako u javnom, tako i u privatnom sektoru, a koji podriva ukupni nivo zaštite cyber prostora, ranjivost na prijetnje i napade, te nemogućnost pravovremenog djelovanja, saradnje i koordinacije sa ostalim državama u regiji i svijetu. Bosna i Hercegovina je jedina zemlja u Evropi koja nema uspostavljen CSIRT sistem (sistem pomoći korisnicima interneta u Bosni i Hercegovini u primjeni proaktivnih mjera za smanjivanje rizika od kompjutersko-

[3] Dokumenti: Konvencija o kibernetičkom kriminalu (Convention on Cybercrime), Budimpešta, 23.11.2001. godine, stupila na snagu 01.07.2004. godine, stupila na snagu u odnosu na BiH 01.09.2006. g; objava „Službeni glasnik BiH“– Međunarodni ugovori broj: 06/2006); Dodatni protokol uz Konvenciju o kibernetičkom kriminalu, o inkriminiranju djela rasističke i ksenofobne naravi počinjenih pomoću računarskih sistema (Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, Strasbourg, 28.01.2003. godine, stupio na snagu 01.03.2006. g, stupio na snagu u odnosu na BiH 01.09.2006. godine; objava „Službeni glasnik BiH“ - Međunarodni ugovori broj: 06/2006);
[4] Izvještaj o rezultatima godišnje ankete korisnika RAK dozvola za pružanje internet usluga u Bosni i Hercegovini za 2018. godinu - procjenjuje se da je u 2018.godini bilo 3,195,294 korisnika Interneta, odnosno da stopa korištenosti interneta u Bosni i Hercegovini za 2018. godinu iznosi 90,49%. Dostupno na: https://docs.rak.ba//documents/ea9d822c-b1dc-4ad9-b2d9-735dc6c8ea91.pdf
[5] CERT (eng. Computer Emergency Response Team) ili CSIRT (engl. Computer Security Incident Response Team)

sigurnosnih incidenata te pružanje pomoći u suzbijanju posljedica nastalih kompjutersko-sigurnosnih incidenata).[6]

U svjetlu opredijeljenosti za buduće članstvo u EU, Bosna i Hercegovina treba da usvoji novu legislativu i usaglasi postojeće zakonodavstvo u oblasti cyber sigurnosti. Vodeći dokumenti su Opća uredba EU o zaštiti podataka[7] i Direktiva Evropskog parlamenta i Evropskog vijeća u vezi sa mjerama za visoki zajednički nivo sigurnosti mrežnih i informacionih sistema u cijeloj Evropskoj uniji („NIS direktiva"). Iako propisi EU ukazuju u kom pravcu treba da idu budući napori, Mjere OSCE-a za izgradnju povjerenja u cyber prostoru[8], već su politički obavezujuće za Bosnu i Hercegovinu.

Zaštita od globalne opasnosti treba da bude sveobuhvatna i usklađena. Da bi se osigurala usklađenost djelovanja, neophodno je imati strateški okvir. Strateški okvir za cyber sigurnost daje smjernice djelovanja svim akterima, te uključuje i administrativne i tehničke aspekte cyber zaštite, definiše viziju i ciljeve koji se njegovom provedbom ostvaruju. Na osnovu smjernica za strateški okvir i budućih izvedenih strategija moguće je kreirati usklađene akcione planove, čijom provedbom će se ostvariti zacrtani ciljevi, odnosno smanjiti rizik po cyber sigurnost.

Ovaj strateški okvir je primijenio pozitivna iskustva i dobre prakse zemalja koje su već usvojile i primjenjuju nacionalne strategije u oblasti cyber sigurnosti. Dokument definiše minimalan broj ciljeva i aktivnosti koji će dovesti do efikasnog i provodivog strateškog okvira, odnosno do konkretnih i mjerljivih rezultata upravljanja sistemom cyber sigurnosti. Takvo upravljanje će se ogledati u provođenju faza u okviru životnog ciklusa projekta, koje se odnose se na: izradu, implementaciju, evaluaciju i prilagođavanje strateškog okvira. Time ovaj dokument predstavlja strateški okvir uspostave efikasnog sistema za cyber sigurnost. Strateški okvir je baziran na NIS direktivi, te vodiču najboljih praksi ENISA-e, kao i na pozitivnim praksama zemalja EU, te zemalja iz okruženja koje su već ranije donijele nacionalne strategije i uspostavile odgovarajuće mehanizme kao odgovor na cyber napade.

Ovaj dokument je urađen u okviru neformalne radne grupe eksperata iz različitih administrativnih nivoa i oblasti djelovanja u Bosni i Hercegovini, okupljene pod okriljem Misije OSCE-a u Bosni i Hercegovini. Prvobitni cilj bavljenja temama prijetnji i zaštite u digitalnom svijetu i započinjanja sveobuhvatne diskusije o strateškom okviru i smjernicama sigurnosti, rezultirao je, kroz izraženu potrebu svih aktera, konkretnim prijedlogom, odnosno dokumentom koji predstavlja strateške

[6] ENISA, CSIRTs by Country - Interactive Map, dostupno na: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map.
[7] (hrv.) UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka); Dostupno na: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1552662547490&uri=CELEX%3A32016R0679
[8] OSCE DECISION No. 1202 OSCE Confidence-Building Measures to Reduce The Risks of Conflict Stemming From The Use of Information And Communication Technologies; PC.DEC/1202, od 10. marta 2016.; dostupno na: https://www.osce.org/pc/227281?download=true

smjernice za harmonizaciju postojećih i izradu budućih strategija za sigurnost cyber prostora u BiH, a što je i u skladu sa preporukama i zaključcima OSCE-ove 11. Pregledne konferencije o ispunjavanju sigurnosnih obaveza Bosne i Hercegovine prema OSCE-u i UN-u .

Dokument je predmet stalne analize, procjene i nadogradnje u skladu sa ciklusima izrade i implementacije strateških ciljeva u cyber domenu.

II. Obim i ciljevi

OBIM

Sektori društva koje obuhvata Strateški okvir za cyber sigurnost u Bosni i Hercegovini su:

1. Institucije vlasti, javni sektor i tijela koja na različite načine predstavljaju korisnike cyber prostora i obaveznike primjene mjera koje proizlaze iz Strateškog okvira.
2. Privatni sektor - pravne osobe koje su obaveznici posebnih propisa o kritičnim informaciono-komunikacionim infrastrukturama, kao i sve druge pravne osobe, odnosno poslovne subjekte koji na različite načine predstavljaju korisnike cyber prostora i obaveznike primjene mjera koje proizlaze iz Strateškog okvira.
3. Građanstvo koje predstavlja korisnike komunikacijskih i informacijskih tehnologija i usluga i na koje se na različite načine reflektira stanje sigurnosti u cyber prostoru. Strateški okvir se odnosi i na one građane koji ne koriste cyber prostor aktivno, ali se njihovi lični podaci nalaze u njemu.

CILJEVI

Opšti cilj

Opšti cilj definisan ovim dokumentom je da se unaprijedi sigurnost cyber prostora u funkciji napretka društva u cjelini. Ovaj cilj, odnosno sigurniji cyber prostor ostvaruje se jačanjem kapaciteta i razvojem mehanizama za prevenciju, detekciju i odgovore na sigurnosne izazove.

Strateški ciljevi:

A. **Osiguran sistematski pristup harmonizaciji i izradi zakonodavstva u oblasti cyber sigurnosti;**
B. **Zaštićeni informaciono-komunikacioni sistemi za pružanje ključnih usluga;**
C. **Podizanje nivoa svijesti i znanja o cyber sigurnosti;**
D. **Uspostavljena tijela zadužena za osiguranje, jačanje i poboljšanje cyber sigurnosti;**
E. **Poboljšana sigurnost i otpornost informaciono-komunikacionih sistema;**
F. **Ojačani kapaciteti za borbu protiv cyber kriminala;**
G. **Uspostavljena efikasna saradnja u oblasti cyber sigurnosti u međunarodnim, regionalnim i domaćim okvirima;**
H. **Izgrađeni kapaciteti za adekvatan odgovor na krizne situacije;**
I. **Uspostavljeno javno-privatno partnerstvo.**

Strateški ciljevi provode se kroz odgovarajuće legislativne, regulatorne i operativne mjere sa ciljem dostizanja i održavanja visokog nivoa sigurnosti informaciono-komunikacionih sistema. Svaki od navedenih strateških ciljeva, obrazložen je podciljevima i razrađen do nivoa aktivnosti potrebnih za njegovu realizaciju.

Strategije za cyber sigurnost koje bi se usvojile na svim nivoima vlasti, u skladu sa ustavnim i zakonski definisanim nadležnostima, treba minimalno da sadrže navedene strateške ciljeve.

Slika 2.

CILJ A: Osiguran sistematski pristup harmonizaciji i izradi zakonodavstva u oblasti cyber sigurnosti

Zakonodavstvo je osnova na kojoj se grade mjere zaštite i definišu obaveze za sve učesnike u sistemu cyber sigurnosti. U cyber sigurnosti okolnosti se brzo mijenjaju, pa je potrebno osigurati da se i zakonodavstvo dovoljno brzo prilagođava ovim promjenama. Promjene treba da budu usklađene i provedene na svim administrativnim nivoima, od zakona do podzakonskih akata.

A1: Urađen pregled postojećeg zakonodavstva, politika, regulativa i mogućnosti

Prvi korak, prije bilo kakvih izmjena, je pregled šta postojeća zakonska rješenja nude u cyber sigurnosti. Osim zakona direktno vezanih za cyber sigurnost, mogu postojati i neki koji se odnose na opštu sigurnost, elektronske komunikacije, ključne usluge i kritičnu infrastrukturu koji regulišu pitanja cyber sigurnosti za neke sektore. Uz zakone mogu postojati i politike i strategije koje se odnose na cyber sigurnost. Sektori koji imaju regulatorna tijela mogu imati svoje propise koji također mogu definisati neka pitanja iz oblasti cyber sigurnosti. Svi takvi postojeći elementi treba da budu iskorišteni za provođenje mjera za poboljšanje stanja cyber sigurnosti odmah, bez čekanja na nove, još neizrađene zakone ili izmjenu postojećih. Tek po uspostavljanju cjelovite slike legislative iz oblasti cyber sigurnosti treba pristupiti harmonizaciji i izmjenama, tamo gdje su potrebne, po prioritetima i u skladu sa nadležnostima.

Aktivnosti kojima se ostvaruje prethodno navedeno su sljedeće:

1. Napraviti pregled postojećih politika vezanih za cyber sigurnost u BiH;
2. Napraviti pregled postojeće regulative vezane za cyber sigurnost u BiH;
3. Napraviti analizu šta postojeće politike i regulativa već omogućavaju iz oblasti cyber sigurnosti.

A2: Usklađeno zakonodavstvo sa međunarodnim propisima, obavezama i standardima u oblasti cyber sigurnosti

Za oblast cyber sigurnosti postoji veći broj međunarodnih propisa u oblasti zakonodavstva, kao i standarda koji mogu biti od pomoći i sa kojim je dobro imati usklađeno zakonodavstvo, pa makar i ne postojala trenutna formalna obaveza. Standardi koji se odnose na cyber sigurnost, a koje izrađuju međunarodna tijela poput ISO, ITU, ENISA, NIST i drugih, rezultat su dugotrajnih procesa i prikupljenih iskustava. Ta prikupljena znanja i iskustva je potrebno koristiti za opšte dobro i sigurnost. Postojeća legislativa iz oblasti cyber sigurnosti, utvrđena tokom procesa pregleda, treba biti analizirana sa aspekta usklađenosti sa međunarodnim propisima i standardima, posebno vodeći računa o obavezama koje su preuzete kroz potpisane međunarodne ugovore, te buduće obaveze koje će biti aktuelne u okviru predpristupnih pregovora Bosne i Hercegovine sa Evropskom unijom. Neusklađenosti treba utvrditi i gdje je moguće otkloniti. Ovo treba da bude prvi korak tokom izmjena postojeće legislative. Neki od standarda pokrivaju samo određene oblasti, pa ih tako treba i primjenjivati i na njih se pozivati prilikom analize legislative iz te oblasti. Neophodno je pratiti izradu definisanog skupa legislative i standarda i usklađivati domaću legislativu i standarde s nastalim promjenama.

Aktivnosti kojima se ostvaruje prethodno navedeno su sljedeće:

1. Definisati skup međunarodnih tijela ili njihovih organizacionih jedinica sa čijim se propisima, obavezama ili standardima treba usklađivati;
2. Definisati skup cyber sigurnosnih propisa, obaveza ili standarda sa kojim se treba usklađivati generalno i pojedinačno po sektorima;
3. Analizirati usklađenosti sa međunarodnim propisima, obavezama ili standardima u domaćem zakonodavstvu;
4. Izraditi neophodna zakonska rješenja usklađena sa međunarodnim obavezama i standardima i otkloniti neusklađenosti u postojećim, a u skladu sa nadležnostima;
5. Stalno pratiti izmjene međunarodnih obaveza i standarda i usklađivati se sa njima.

A3: Uravnotežena sigurnost sa privatnošću i zaštitom podataka

Provođenje mjera zaštite cyber sigurnosti ne smije ugroziti privatnost građana koja predstavlja osnovno ljudsko pravo i slobodu. Svi građani imaju pravo na privatnost i zaštitu ličnih podataka. O

ovome je neophodno povesti računa prilikom donošenja novih i izmjena postojećih zakona, kao i prilikom planiranja i provođenja mjera zaštite.

Aktivnosti kojima se ostvaruje prethodno navedeno su:

1. U svim koracima provođenja strategije voditi računa o privatnosti i zaštiti ličnih podataka u skladu sa međunarodnim standardima kao i Opštom uredbom o zaštiti podataka EU (GDPR).

CILJ B: Zaštićeni informaciono-komunikacioni sistemi za pružanje ključnih usluga

Informaciono-komunikacioni sistemi koji omogućavaju pružanje usluga ključnih za održavanje kritičnih društvenih i ekonomskih aktivnosti, treba da budu posebno zaštićeni. Skup ključnih usluga i baza podataka od kritičnog značaja, spisak operatora ključnih usluga i baza podataka i kritična informaciono-komunikaciona infrastruktura trebaju biti zakonski definisani. Uz definiciju treba biti propisana obaveza zaštite kritične informaciono-komunikacione infrastrukture operatorima ključnih usluga i baza podataka. Za sve operatore ključnih usluga i baza podataka potrebno je propisati minimalne sigurnosne mjere koje je potrebno poduzeti. Ove mjere treba da budu u skladu sa cyber sigurnosnim standardima za sektor kojem taj operator pripada. Svaki od operatora ključnih usluga i baza podataka treba poduzeti mjere smanjivanja rizika po kritičnu informaciono-komunikacionu infrastrukturu. Ove mjere treba da budu rezultat provedene analize u skladu sa propisanom metodologijom analize rizika. Operatorima ključnih usluga i baza podataka potrebno je propisati obavezu redovne provedbe analize rizika. Također, operatori ključnih usluga treba da imaju svoje CSIRT-ove koji sarađuju sa drugim CSIRT-ovima i tijelima definisanim u cilju D u skladu sa NIS Direktivom.

B1: Zakonski definisane ključne usluge i baze podataka, njihovi operatori i kritična informaciono-komunikaciona infrastruktura te obaveza njene zaštite.

Ključne usluge i baze podataka treba da budu definisane zakonskim okvirom. Za svaku od ključnih usluga i baza podataka potrebno je u zakonu utvrditi operatore koji je pružaju i sudionike odgovorne za sigurnost ključnih usluga i baza podataka. Zaštita informaciono-komunikacione infrastrukture ovih operatora od koje zavisi funkcionisanje ključnih usluga i baza podataka treba biti zakonski obavezna.

Aktivnosti:

1. Donošenje legislative o ključnim uslugama i bazama podataka, operatorima ključnih usluga i kritičnoj informaciono-komunikacionoj infrastrukturi;

2. Propisivanje obaveze zaštite kritične informaciono-komunikacione infrastrukture operatorima ključnih usluga.

B2: Utvrđene minimalno potrebne sigurnosne mjere

Operatori ključnih usluga koje pripadaju istom sektoru ili pružaju istu ključnu uslugu treba da imaju usklađen pristup u cyber zaštiti. Taj pristup treba biti zasnovan na opštim međunarodnim cyber sigurnosnim standardima, a posebno onim koji se koriste u tom sektoru. Na taj način omogućava se međusobno razumijevanje, provjera provođenja mjera od nadležnih organa i razmjena informacija o dobrim sigurnosnim praksama i sigurnosnim incidentima. Definisanjem minimalno potrebnih sigurnosnih mjera omogućava se racionalna i usmjerena upotreba ograničenih resursa. Ove mjere mogu biti definisane u zakonu koji tretira ključne usluge i njihove operatore.

Aktivnosti:

1. Analiza minimalno potrebnih sigurnosnih mjera po sektorima – ključnim uslugama;
2. Usklađivanje sa međunarodnim sigurnosnim standardima za sektor;
3. Ažuriranje legislative po potrebi.

B3: Smanjen rizik i posljedice po kritičnu infrastrukturu od napada ili nesreća

Smanjivanjem rizika smanjuje se mogućnost ugrožavanja sigurnosti i njene posljedice. Kako bi se rizik smanjio, neophodno je provesti njegovu analizu. Analiza rizika je obiman i složen proces. Da bi se pomoglo operatorima ključnih usluga i baza podataka, te osigurao usklađen pristup, potrebno je usvojiti metodologiju koja se treba koristiti za analizu rizika po ključnim uslugama i sektorima u skladu sa nadležnostima. Svaki operator treba znati koju proceduru provoditi da bi njegova analiza rizika bila kompletna. Svaki operator identificira svoje informaciono-komunikacione sisteme čijim bi ugrožavanjem bilo ugroženo pružanje ključnih usluga za koje je operator nadležan. Nad tim sistemima treba provesti analizu rizika. Na osnovu te analize operatori poduzimaju mjere za smanjenje rizika. Cjelokupan proces analize rizika treba biti dokumentovan i obavljan redovno u minimalno propisanim razmacima.

Aktivnosti:

1. Usvojiti metodologije analize rizika za sve operatore ključnih usluga i baza podataka po ključnim uslugama i sektorima u skladu sa nadležnostima;
2. Svaki operator treba identificirati informaciono-komunikacionu infrastrukturu koja je kritična za pružanje ključnih usluga za koje je on odgovoran;
3. Procijeniti rizik od ugrožavanja sigurnosti svih dijelova prethodno identifikovanih informaciono-komunikacionih sistema, poredati ih po negativnom utjecaju koji mogu imati i izračunati vjerovatnoću dešavanja;

4. Odlučiti koje rizike umanjiti i kojim mjerama, koje prihvatiti i za koje ne treba poduzimati nikakve mjere (nepoduzimanje mjera obavezno obrazložiti);
5. Napraviti registar identifikovanih rizika;
6. Propisati redovnu obavezu stalnog nadzora slabosti i prijetnji, te ažuriranja informacija o time izazvanim promjenama rizika.

CILJ C: Podizanje nivoa svijesti i znanja o cyber sigurnosti

Za ostvarivanje svih strateških ciljeva, a posebno onog koji se odnosi na podizanje svijesti i nivoa obrazovanja, neophodno je poduzeti mjere kojim će se proširiti informacije o potrebi zaštite informacija i informaciono-komunikacione infrastrukture. Ove mjere će podići opšti nivo obrazovanja građanstva iz ove oblasti, smanjiti odliv stručnog kadra, te povećati broj kompetentnih lica koja mogu dizajnirati i provoditi mjere zaštite.

C1: Podizanje svijesti o cyber sigurnosti

Preduslov za provođenje bilo koje strategije je podrška institucija i pojedinaca koji donose odluke. Donosioci odluka treba da shvate potrebu donošenja i provođenja strategije cyber sigurnosti. Ovo shvatanje treba da se zasniva na dobroj informisanosti i razumijevanju problema koji se rješava. Za to nije potrebno tehničko poznavanje informaciono-komunikacionih sistema. Dovoljno je biti svjestan da sigurnost informacija i informaciono-komunikacione infrastrukture može biti ugrožena, a što može rezultirati katastrofalnim posljedicama, te da postoje mjere kojima se rizik od takvih dešavanja može smanjiti. Osim donosilaca odluka sve osobe koje dolaze u dodir sa podacima koji se smatraju kritičnim i koji rade na kritičnoj informaciono-komunikacionoj infrastrukturi treba da imaju svijest o potrebi zaštite ovih podataka i infrastrukture. Svijest društva o cyber sigurnosti bitna je za prihvatanje i provođenje mjera sigurnosti informacija na svim mjestima, na svim nivoima i u svim vremenskim okvirima. Društvo koje postigne nivo opšte informisanosti biće sigurnije društvo.

Aktivnosti:

1. Redovno informisati donosioce odluka o cyber sigurnosti, sigurnosno relevantnim događajima iz prošlosti i njihovim posljedicama, te mogućim budućim posljedicama neprovođenja mjera zaštite;
2. Uvesti cyber sigurnost kao obavezan program obuke uposlenika operatora ključnih usluga i baza podataka od kritičnog značaja, kao i uposlenika institucija javne uprave;
3. Provoditi kampanje putem medija, uključujući i društvene mreže, radi podizanja nivoa svijesti o potrebi cyber sigurnosti;

4. Podržavati procese uključivanja medijske i informacijske pismenosti u formalno i neformalno obrazovanje.

C2: Jačanje programa treninga i obrazovanja

Osim podizanja svijesti svih aktera o cyber sigurnosti bitno je podići i nivo specijalističkih znanja iz ove oblasti kako među profesionalcima, tako i u sklopu opšte populacije. To se može postići kroz formalno, neformalno i cjeloživotno učenje. Bosna i Hercegovina treba da poveća broj stručnjaka iz cyber sigurnosti, ako se želi uspješno zaštititi od cyber opasnosti. Da bi se to postiglo potrebno je uvesti specijalističke studije iz ove oblasti u škole i univerzitete u Bosni i Hercegovini. Osim toga, potrebno je uvesti redovno stručno usavršavanje svih osoba nadležnih za tehničke aspekte sigurnosti informacija u svim institucijama na svim nivoima. Posebne obuke koje provode proizvođači za rad sa opremom i softverom, a koji se koriste u nekoj instituciji, treba da budu obavezne za službenike koji rade sa njima. Uz obrazovanje profesionalaca cyber sigurnosti potrebno je podići nivo znanja iz ove oblasti među građanstvom. To je proces koji treba provoditi kroz cjelokupno obrazovanje od osnovne škole do fakulteta. Na ovaj način se podiže ukupni nivo znanja i sigurnosti cijelog društva.
Aktivnosti:

1. Uvoditi specijalističke studije i programe cyber sigurnosti na univerzitetima;
2. Uvoditi obavezne specijalističke treninge cyber sigurnosti za rad sa platformama koje se koriste u institucijama javne uprave;
3. Uvoditi teme vezane za cyber sigurnost i medijsku i informacijsku pismenost u nastavne planove svih nivoa obrazovanja.

C3: Stimulacija zapošljavanja IKT kadrova u javnom sektoru

Ispravno funkcionisanje informaciono-komunikacionih sistema, kao i njihova sigurnost, oslanja se na kvalifikovane IKT kadrove. Savremeno tržište rada ovim kadrovima nudi velika primanja. Institucije uglavnom imaju definisane platne razrede koji ne omogućavaju plaćanje IKT kadrova po tržišnim cijenama. Iz ovog razloga IKT kadrovi odlaze u privatne firme ili odlaze van zemlje. Neophodno je iznaći način da se ovaj proces zaustavi. To se može ostvariti promjenama u načinu obračuna primanja kvalifikovanih IKT kadrova u institucijama, dodatnim mogućnostima usavršavanja, te stimulativnim radnim okruženjem.

Aktivnosti:

1. Adekvatno vrednovati rad IKT kadrova;
2. Omogućiti stalno usavršavanje IKT kadrovima;
3. Promovisati izazove rada na velikim informaciono-komunikacionim sistemima.

C4: Stimulacija istraživanja i razvoja

Istraživanje i razvoj omogućavaju predviđanje mogućih cyber opasnosti, te sprečavanje istih. Istraživanje i razvoj treba biti rađeno organizovano sa fokusom na oblastima cyber sigurnosti koje su specifične za Bosnu i Hercegovinu. Istraživanje i razvoj traže ulaganja koja je neophodno planirati u budžetima institucija i ministarstava nadležnih za nauku. Akademska zajednica treba da aktivnije sarađuje sa institucijama i privredom. Naučnoistraživački i stručni projekti osnova su istraživanja i razvoja. Potrebno je uložiti napore za uključivanje u međunarodne projekte. Da bi se ostvario kvalitet za uključivanje u kompetitivne međunarodne projekte neophodno je prvo uložiti u domaće projekte kroz koje će se razviti kompetencije i objaviti radovi na osnovu koji će naši istraživači biti prepoznati u istraživačkoj zajednici. Potrebno je stimulisati aktivnije učešće na naučnim i stručnim konferencijama. Na taj način se razmjenjuju iskustva i priprema za izazove koji dolaze.

Aktivnosti:

1. Stimulisati ulaganja u naučnoistraživački rad iz oblasti cyber sigurnosti;
2. Definisati specifične oblasti cyber sigurnosti na čije istraživanje se treba fokusirati;
3. Stimulisati učešće u međunarodnim naučnoistraživačkim projektima iz cyber sigurnosti;
4. Stimulisati učešće istraživača na konferencijama posvećenim cyber sigurnosti;
5. Stimulisati saradnju akademske zajednice sa institucijama.

CILJ D: Funkcionalna tijela zadužena za osiguranje, jačanje i poboljšanje cyber sigurnosti

Radi usklađene borbe protiv cyber opasnosti potrebno je imati tijela zadužena za to. Ta tijela treba da imaju jasno definisane nadležnosti koje su u skladu sa teritorijom i sektorom u kom djeluju. Prilikom uspostavljanja ovih tijela potrebno se držati međunarodnih standarda i pravila, a pogotovo onih iz EU. NIS direktiva nalaže članicama EU obaveze iz ove oblasti, pa je i ovaj strateški okvir usklađen sa zahtjevima iz NIS direktive. Potrebno je imenovati nadležna tijela, kontaktnu tačku i CSIRT-ove čiji su zadaci vezani uz sigurnost informaciono-komunikacionih sistema.

D1: Imenovana nadležna tijela za sigurnost informaciono-komunikacionih sistema

Potrebno je imenovati nadležna tijela u Bosni i Hercegovini za sigurnost informaciono-komunikacionih sistema koja obuhvataju barem sektore i usluge iz Priloga I. Nadležna tijela treba da imaju odgovarajuće resurse za izvršavanje dodijeljenih obaveza. Nadležna tijela, kad god je to potrebno i u skladu s važećom legislativom, savjetuju se s nadležnim institucijama i organima za provođenje zakona, te tijelima za zaštitu podataka, te s njima sarađuju.

Aktivnosti:

1. Utvrditi potrebna tijela i njihove nadležnosti;
2. Uspostaviti nadležna tijela sa odgovarajućim ljudskim i materijalnim resursima.

D2: Uspostavljena kontakt tačka

Potrebno je uspostaviti kontakt tačku za sigurnost informaciono-komunikacionih sistema u skladu s NIS Direktivom i ustavnim i zakonskim nadležnostima. Kontakt tačka izvršava funkciju povezivanja s ciljem osiguravanja međunarodne saradnje nadležnih tijela u Bosni i Hercegovini s relevantnim tijelima u drugim državama.

Aktivnosti:

1. Uspostaviti kontakt tačku u skladu s NIS Direktivom
2. Osigurati odgovarajuće ljudske i materijalne resurse za kontakt tačku.

D3: Uspostavljeni potrebni CSIRT-ovi

Potrebno je imenovati CSIRT-ove koji udovoljavaju zahtjevima iz tačke 1. Priloga III i koji obuhvataju minimalno sektore i usluge iz Priloga I. odgovornih za smanjivanje rizika i sprečavanje ili otklanjanje posljedica incidenata u skladu s tačno propisanim postupkom. CSIRT se može osnovati unutar nadležnog tijela. Imenovanim CSIRT-ovima potrebno je osigurati odgovarajuće resurse za efektivno izvršavanje zadataka iz tačke 2. Priloga III. Potrebno je omogućiti efektivnu i sigurnu saradnju CSIRT-ova. Za komunikaciju i informisanje CSIRT-ovi trebaju pristup prikladnoj, sigurnoj i otpornoj infrastrukturi.

Aktivnosti:

1. Utvrditi potrebne CSIRT-ove i njihove nadležnosti;
2. Uspostaviti i jačati kapacitete CSIRT-ova u ljudskom, tehničkom, operativnom i institucionalnom smislu;
3. Uspostaviti prikladnu, sigurnu i otpornu infrastrukturu za komunikaciju CSIRT-ova.

CILJ E: Poboljšana sigurnost i otpornost informaciono-komunikacionih sistema

Osim kritične informaciono-komunikacione infrastrukture kod operatora ključnih usluga i baza podataka neophodno je zaštititi i javnu informaciono-komunikacionu infrastrukturu. Operatori ove infrastrukture su svi nositelji dozvola koje izdaje Regulatorna agencija za komunikacije Bosne i Hercegovine. To uključuje davaoce usluge pristupa Internetu (eng. ISP), mobilnoj i fiksnoj telefoniji, te mrežne operatere. Ovi operatori treba da imaju zakonski propisanu obavezu provođenja cyber zaštite svojih sistema. Da bi se osiguralo provođenje zaštite, neophodno je definisati minimalno potrebne mjere

zaštite i parametre čijim se nadzorom kontroliše provođenje zaštite. Operatore treba obavezati da koriste neutralnu tačku za razmjenu internetskog saobraćaja (IXP) za saobraćaj između institucija, te stimulisati da je koriste za sav saobraćaj unutar BiH. Privatne operatore treba stimulisati da ulažu u cyber zaštitu.

E1: Zakonski definisana obaveza provođenja zaštite javne informaciono-komunikacione infrastrukture za sve javne i privatne operatore

Regulatorna agencija za komunikacije, kao tijelo nadležno za nosioce dozvola za pružanje komunikacionih usluga, treba osigurati da operatori komunikacionih usluga imaju zakonsku obavezu provođenja cyber zaštite svojih sistema.

Aktivnosti:

1. Analizirati postojeću regulativu zaštite javne informaciono-komunikacione infrastrukture;
2. Propisati (zakonsku) obavezu zaštite javne informaciono-komunikacione infrastrukture za javne i privatne operatore.

E2: Omogućen tehnički nadzor mjera zaštite operatora javnih informaciono-komunikacionih sistema i savjetovanje o mjerama

Regulatorna agencija za komunikacije treba propisati sigurnosne zahtjeve koje operatori treba da ispunjavaju i koji se mogu nadzirati. Ti zahtjevi minimalno treba da uključe međunarodne cyber sigurnosne standarde koje operatori treba da poštuju. Osim toga, potrebno je regulisati zaštitu privatnosti korisnika, obavezu informisanja o sigurnosnim incidentima i saradnje sa drugim operatorima i agencijama za provođenje zakona u incidentnim situacijama.

Aktivnosti:

1. Definisati sigurnosno relevantne parametre nadzora i kontrole;
2. Omogućiti kontinuiran nadzor sigurnosno relevantnih parametara;
3. Provoditi redovne preglede rada operatora javne informaciono-komunikacione infrastrukture.

E3: Neutralna tačka za razmjenu internetskog saobraćaja (IXP) koristi se za saobraćaj između institucija

Upotreba neutralne tačke za razmjenu internetskog saobraćaja (IXP) eliminiše nepotrebno putovanje internet saobraćaja, između dva korisnika u zemlji, preko ISP-a iz drugih zemalja. Ovo smanjuje sigurnosne rizike po podatke i snižava troškove za ISP. Bosna i Hercegovina ima uspostavljen jedan IXP u Univerzitetskom tele-informatičkom centru (UTIC) Univerziteta u Sarajevu, ali ih u budućnosti može biti i više. ISP-ovi treba da se obavežu, da saobraćaj između institucija u Bosni i Hercegovini koje koriste različite ISP-ove, isključivo putuje preko IXP-a, a nikad van zemlje. Izuzetak od ovog pravila čini saobraćaj ka odobrenim davaocima usluga *cloud computing* koje ove institucije

koriste. Za ISP-ove je uglavnom efikasnije i ekonomičnije da koriste IXP za sve svoje korisnike, a ne samo za institucije i to treba ohrabrivati.

Aktivnosti:

1. Obavezati ISP-ove institucija da saobraćaj prema drugim institucijama koje nisu njihovi korisnici usmjeravaju isključivo preko IXP-a, osim saobraćaja ka odobrenim davaocima usluga *cloud computing* van Bosne i Hercegovine.

E4:Definisan siguran način upotrebe usluga *cloud computing*

Cloud computing omogućava racionalnu i ekonomičnu upotrebu računarskih resursa. U slučaju upotrebe usluga *cloud computing* podaci se šalju i obrađuju van organizacije koja je njihov vlasnik. Mjesto obrade može biti i u drugoj državi. Ovo otvara pitanje provođenja sigurnosti ovakvih podataka i odgovornosti. Da bi se osigurao potreban nivo sigurnosti potrebno je koristiti samo davaoce usluga *cloud computing* koji imaju certifikate da zadovoljavaju međunarodne sigurnosne standarde, a posebno one koji se odnose na *cloud* sigurnost. Primjeri ovakvih standarda su porodica ISO 27000 standarda, a posebno ISO27017 fokusiran na *cloud*. Potrebno je razmotriti da li postoje podaci koji se ne bi smjeli slati u *cloud* ili u *cloud* van Bosne i Hercegovine. Takve podatke bi trebalo definisati i osigurati da se za njih ne koristi *cloud*, odnosno *cloud* van Bosne i Hercegovine.

Aktivnosti:

1. Definisati minimalni skup sigurnosnih standarda koje davaoci usluga *cloud computing* treba da ispunjavaju;
2. Koristiti samo one davaoce usluga *cloud computing* koji zadovoljavaju utvrđene standarde;
3. Razmotriti da li postoje podaci koji se ne bi smjeli uopšte slati na *cloud* ili se ne bi smjeli slati na *cloud* van Bosne i Hercegovine i ako postoje odrediti koji su;
4. Za podatke za koje je to utvrđeno kao nedozvoljeno provesti sprečavanje slanja na *cloud* ili na *cloud* van Bosne i Hercegovine.

E5: Stimulisan privatni informaciono-komunikacioni sektor za investiranje u sigurnosne mjere

Privatni operatori treba da vode računa da njihova ulaganja imaju ekonomsku opravdanost. Iako se ulaganja u cyber sigurnost dugoročno isplate, inicijalna ulaganja mogu predstavljati preveliko kratkoročno finansijsko opterećenje. Iz ovog razloga potrebno je pronaći odgovarajuće načine stimulisanja privatnih operatora za ova ulaganja. To može biti kroz određene olakšice za potrebne nabavke namijenjene povećanju cyber sigurnosti. Poželjno bi bilo uspostaviti istraživačke fondove i centre cyber sigurnosti koji bi pomagali i privatnim operatorima. Potrebno je razviti kapacitete za pomoć

i privatnim operatorima prilikom sigurnosnih incidenata. Ovo treba uključivati pomoć pri oporavku podataka i forenzičkoj analizi incidenta.

Aktivnosti:

1. Razmotriti mogućnost uvođenja olakšica za operatore komunikacionih usluga za ulaganja u cyber sigurnost;
2. Omogućiti privatnim operatorima komunikacionih usluga pristup rezultatima istraživanja iz cyber sigurnosti koja su finansirana iz javnih fondova;
3. Pružati podršku operatorima komunikacionih usluga nakon cyber incidenata.

CILJ F: Ojačani kapaciteti za borbu protiv cyber kriminala

Konstantno usavršavanje i porast sofisticiranosti cyber kriminala i cyberom omogućenog kriminala, kao i metoda i tehnika kojima se cyber kriminal izvodi, zahtijeva kontinuirano jačanje kapaciteta u cilju efikasnog odgovora na cyber kriminal. Cyber kriminal i elektronski dokazni materijal zahtijevaju specijalizovani odgovor nadležnih institucija za provođenje zakona. Ove institucije i pravosudni sistem treba da su u mogućnosti da sprovode istrage i procesuiraju djela iz oblasti cyber kriminala i cyberom omogućenog kriminala, te da koriste elektronski dokazni materijal koji se odnosi na bilo koje krivično djelo. Cyber kriminal i cyberom omogućen kriminal treba biti adekvatno tretiran u zakonodavstvu. Nadležne institucije za provođenje zakona treba da imaju adekvatne ljudske i materijalne resurse. Tužilaštva i sudovi treba da budu upoznati i adekvatno obučeni o savremenom cyber kriminalu.

F1: Konstantan razvoj zakonodavstva u oblasti cyber kriminala i cyberom omogućenog kriminala

Uporedo sa brzim tehnološkim razvojem pojavljuju se i nove vrste krivičnih djela. Različiti oblici cyber kriminala mogu biti neprepoznati u zakonodavstvu. Time se otvara mogućnost da neka djela ne budu zakonski kvalifikovana. Nadležne institucije za provođenje zakona i pravosudni sistem tada nemaju uporište za poduzimanje akcija za sprečavanje ovih djela i sankcionisanje počinilaca. Iz ovog razloga je neophodno redovno pratiti nove pojavne oblike cyber kriminala i cyberom omogućenog kriminala, te analizirati da li ih postojeće zakonodavstvo prepoznaje. Ukoliko to nije slučaj, potrebno je izmijeniti zakon. Pošto se zakoni mijenjaju sporije nego što se novi oblici cyber kriminala pojavljuju, potrebno je konsultovati stručna lica prilikom izmjena zakona koji pokrivaju ovu oblast.

Aktivnosti kojima se ostvaruje prethodno navedeno su:

1. Redovno analizirati usklađenosti postojećeg zakonodavstva sa savremenim oblicima cyber kriminala;
2. Razvijati zakonodavstvo u skladu s rezultatima analiza.

F2: Razvijeni ljudski i tehnički kapaciteti institucija za provođenje zakona

Brzi razvoj tehnologije omogućava nove oblike kriminala. Za borbu protiv ovih oblika kriminala neophodno je imati adekvatno educirano ljudstvo u institucijama za provođenje zakona. To obrazovanje treba biti konstantno i uključivati tehničke i kriminalističke aspekte. Educirani kadrovi su potrebni, ali sami nisu dovoljni. Neophodno je tehnički opremiti institucije za provođenje zakona opremom i softverom potrebnim za prevenciju, detekciju i obradu djela cyber kriminala. Institucije za provođenje zakona bi trebale imati specijalističke timove za borbu protiv cyber kriminala.

Aktivnosti:

1. Redovno edukovati uposlenike agencija za provođenje zakona iz oblasti cyber kriminala i njegove forenzike;
2. Tehnički opremiti institucije za provođenje zakona potrebnom opremom za borbu protiv cyber kriminala;
3. Unaprijediti kapacitete za digitalnu forenziku;
4. Formirati i ojačavati specijalizovane timove za borbu protiv cyber kriminala u svim nadležnim institucijama za provođenje zakona, u skladu sa strateškom procjenom i iskazanim potrebama;
5. Formirati posebne odjele za cyber kriminal ili u sistematizaciji predvidjeti tužioca/e i sudiju/e za cyber kriminal u nadležnim tužilaštvima i sudovima.

F3: Stalna obuka tužilaca i sudija o savremenom cyber kriminalu

Tužioci i sudije treba da budu upoznati sa savremenim oblicima cyber kriminala i cyberom omogućenog kriminala. Potrebno ih je redovno upoznavati i obučavati sa karakteristikama cyber kriminala koje se razlikuju od klasičnih krivičnih djela. Tužioci i sudije treba da znaju karakteristike i posebnosti elektronskih dokaza. Potrebno je da razumiju bitnost pravovremenog prikupljanja ovih dokaza i njihovu osjetljivost na izmjene. Tužiocima su ova znanja potrebna za adekvatno vođenje istraga cyber kriminala, a sudijama za lakše praćenje izlaganja i ocjenu elektronskih dokaza u slučajevima cyber kriminala.

Aktivnosti:

1. Redovno obučavati tužioce i sudije o savremenom cyber kriminalu;
2. Redovno obučavati tužioce i sudije o elektronskim dokazima.

CILJ G: Uspostavljena efikasna saradnja u oblasti cyber sigurnosti u međunarodnim, regionalnim i domaćim okvirima

Zaštita cyber sigurnosti se treba provoditi sveobuhvatno da bi bila uspješna. Neophodno je uspostaviti efikasnu saradnju po svim sektorima i na svim nivoima, od lokalnog do međunarodnog. Ova saradnja treba da bude u skladu sa nadležnostima. Mehanizmi saradnje treba da budu usklađeni sa zahtjevima iz NIS direktive.

G1: Ostvarena efikasna saradnja u oblasti cyber sigurnosti u domaćim okvirima

Potrebno je osigurati saradnju i razmjenu potrebnih informacija između kontakt tačke, nadležnih tijela i CSIRT-ova. Potrebno je osigurati efikasnu, djelotvornu i sigurnu saradnju svih CSIRT-ova, nezavisno od sektora i teritorije.

Aktivnosti:

1. Osigurati dostavljanje informacija o sigurnosnim incidentima do nadležnih CSIRT-ova;
2. Osigurati CSIRT-ovima pristup informacijama potrebnim za obavljanje njihovih zadataka kod operatora ključnih usluga u skladu sa nadležnostima;
3. Osigurati razmjenu relevantnih informacija između CSIRT-ova i kontakt tačke;
4. Osigurati efikasnu, djelotvornu i sigurnu suradnju svih domaćih CSIRT-ova.

G2: Uključivanje u međunarodnu i regionalnu saradnju

Međunarodna i regionalna saradnja omogućava razmjenu informacija o aktuelnim sigurnosno interesantnim događajima iz oblasti IKT, kao i iz ostalih oblasti. Time se podržava pravovremena i aktuelna priprema i reakcija na moguće napade. Kroz ovu saradnju omogućena je razmjena znanja i stvaranje baze znanja koja ojačava sve učesnike u razmjeni. Uključivanje u međunarodnu saradnju podrazumijeva prihvatanje i provođenje međunarodnih standarda iz oblasti cyber sigurnosti. Međunarodna saradnja omogućava istraživanje i razvoj što doprinosi povećanju znanja iz oblasti cyber sigurnosti. Članstvo Bosne i Hercegovine u UN-u, OSCE-u, Vijeću Evrope, FIRST-u, TF-CSIRT-u i drugim organizacijama, donosi obaveze provođenja usvojenih mjera cyber sigurnosti. Ispunjavanje ovih obaveza donosi pristup resursima ovih organizacija. Minimalni oblik međunarodne saradnje koji je obavezno osigurati je razmjena informacija sa drugim državama i međunarodnim organizacijama putem kontakt tačke.

Aktivnosti:

1. Jačati i širiti saradnju Bosne i Hercegovine sa međunarodnim partnerima unutar organizacija čija je Bosna i Hercegovina članica, poput OSCE-a, Vijeća Evrope i UN-a, te organizacija čijem se članstvu teži, prije svega EU, a posebno saradnju sa zemljama iz regije;
2. Učestvovati u i organizovati međunarodne praktične i teoretske razmjene znanja poput vježbi, obuka, konferencija i seminara iz oblasti cyber sigurnosti;
3. Osigurati adekvatnu razmjenu informacija sa drugim državama i međunarodnim organizacijama.

CILJ H: Izgrađeni kapaciteti za adekvatan odgovor na krizne situacije

Iskustvo je pokazalo da se, i pored svih preventivnih mjera zaštite cyber sigurnosti, mogu desiti situacije u kojima je ugroženo funkcionisanje kritične informaciono-komunikacione infrastrukture, a time i pružanje ključnih usluga. Za takve situacije je neophodna priprema radi smanjivanja njihovog negativnog utjecaja i što bržeg okončanja. Pripreme se sastoje od utvrđivanja procedura ponašanja i obezbjeđivanja potrebnih resursa za odgovor. Prije svega neophodno je precizno definisati šta se smatra kriznom situacijom da bi se omogućila njena identifikacija i prijava prema proceduri koju također treba definisati. Prijava krizne situacije treba pokrenuti pripremljene procedure i operativne planove kod svih relevantnih učesnika. Budući da primarni načini komunikacije mogu biti pogođeni incidentom koji je izazvao kriznu situaciju, potrebno je unaprijed pripremiti alternativne komunikacione kanale. Da bi se navedeno ostvarilo, neophodno je imati adekvatne ljudske i materijalne resurse koji mogu provesti planirane mjere.

H1: Uspostavljeni kriteriji za utvrđivanje krizne situacije

Nadležna tijela treba da operatorima ključnih usluga i baza podataka propišu kriterije za utvrđivanje krizne situacije. Osnovni kriteriji koji treba da se koriste za procjenu koliko neki incident predstavlja kriznu situaciju su: broj korisnika za koje je incident doveo do prekida pružanja ključne usluge; trajanje incidenta; geografska veličina područja na koje bi incident mogao utjecati; obim poremećaja u pružanju usluge i obim utjecaja na ekonomske i društvene aktivnosti.

Aktivnosti:

1. Uspostaviti kriterije za utvrđivanje krizne situacije za sve operatore ključnih usluga i baza podataka.

H2: Uspostavljeni mehanizmi prijave incidenata

Sve sigurnosne incidente na kritičnoj informaciono-komunikacionoj infrastrukturi operatori ključnih usluga i baza podataka obavezni su odmah prijaviti nadležnom CSIRT-u. Nadležni CSIRT radi procjenu težine incidenta i na osnovu te procjene poduzima dalje akcije. Nadležni CSIRT može, ako

procjeni potrebnim, proslijediti informaciju o incidentu do drugih CISRT-ova ili kontakt tačke, te može izdati sigurnosno upozorenje. Sigurnosna upozorenja mogu biti javna za sve građane i institucije ili ciljana prema nadležnom tijelu ili institucijama za provođenje zakona.

Aktivnosti:

1. Obavezati operatore ključnih usluga i baza podataka da incidente na kritičnoj informaciono-komunikacionoj infrastrukturi prijave nadležnom CSIRT-u;
2. Savjetovati operatore ključnih usluga i baza podataka da i ostale incidente prijave nadležnom CSIRT-u;
3. Uspostaviti proceduru procjene težine incidenta u CSIRT-ovima;
4. Uspostaviti proceduru izdavanja sigurnosnih upozorenja;
5. Uspostaviti alternativnu komunikacionu infrastrukturu za slučajeve cyber incidenata.

H3: Izrađeni operativni planovi i procedure postupanja u kriznim situacijama za sve odgovorne institucije

Svi operatori ključnih usluga i baza podataka, svi CSIRT-ovi, sva nadležna tijela i kontakt tačka treba da naprave procedure i operativne planove kojim se definiše način ponašanja i djelovanja u kriznim situacijama. Ove procedure i planovi mogu uključivati i druge institucije, poput nadležnih ministarstava ili regulatora, koje onda takođe treba da imaju svoje procedure i planove za krizne situacije u okviru njihove nadležnosti. Potrebno je imati i proceduru i nadležnost za komuniciranje s javnošću u ovim situacijama. Procedure i operativne planove treba isprobati, najbolje kroz simulaciju cyber napada, te na osnovu rezultata raditi njihovu analizu i ažuriranje.

Aktivnosti:

1. Napraviti procedure i operativne planove za krizne situacije u svim operatorima ključnih usluga i baza podataka, CSIRT-ovima, nadležnim tijelima i kontakt tački, uz neophodni stepen usklađenosti;
2. Definisati institucije koje, osim navedenih, treba uključiti i koje treba da naprave procedure i planove;
3. Utvrditi nadležnost i način komuniciranja s javnošću u kriznim situacijama;
4. Provoditi redovne i zajedničke simulacije cyber napada sa ciljem provjere procedura i operativnih planova;
5. Najmanje jednom godišnje ažurirati procedure i operativne planove za krizne situacije, a po potrebi i vanredno nakon provedenih simulacija cyber napada.
6. Stimulisati uspostavu i razvoj centara za upravljanje kriznim situacijama

H4: Kadrovski i materijalno popunjene organizacije u skladu sa planovima i procedurama za krizne situacije

Na osnovu utvrđenih procedura i planova za krizne situacije potrebno je obučiti odgovorno osoblje i osigurati ostale potrebne resurse za sprovođenje procedura i planova.

Aktivnosti:

1. Obučiti osoblje u skladu sa procedurama i operativnim planovima za krizne situacije;
2. Osigurati potrebne resurse za provođenje procedura i operativnih planova za krizne situacije

CILJ I: Uspostavljeno javno-privatno partnerstvo

Privatni sektor – preduzeća i korporacije u privatnom vlasništvu - predstavljaju bitan element u sferi sektora cyber sigurnosti. Sa ovim kompanijama potrebno je uspostaviti efikasnu i jasno definisanu saradnju i strateška partnerstva o pitanjima vezanim za cyber sigurnost, a na obostranu korist. Evropska legislativa[9] podstiče potrebu za javno-privatnom saradnjom u polju cyber sigurnosti kao i važnost izgradnje povjerenja kroz javno-privatna partnerstva (JPP) [10]. U tom smislu ENISA je objavila dokument „JPP: Modeli saradnje“[11] u kojem se do detalja razvijaju preporučeni i uspješni modeli JPP-a, te identificiraju uspješna postojeća rješenja primjene istih unutar Europske unije.

Javno-privatna partnerstva u smislu industrijskog i akademskog razvoja i inovacije također su vid potrebne i moguće saradnje. Primjer tome je sveobuhvatni JPP ugovor potpisan između Europske unije i mreže Europske Cyber Security Organisation (ECSO)[12].

I1: Uspostavljeno javno-privatno partnerstvo sa preduzećima i korporacijama koje razvijaju i nude proizvode, rješenja i usluge iz domena cyber sigurnosti

Privatne kompanije razvijaju, na tržištu nude i implementiraju sve proizvode (softver i hardver) kao i rješenja zaštite IT sistema i podataka. Takođe, privatna preduzeća i korporacije razvijaju i na tržištu nude usluge cyber sigurnosti, bilo kao integrisane usluge, konsalting ili oboje. Pored toga, dio operatora ključnih usluga su privatne kompanije. Pored velikih globalnih korporacija koje ove usluge uspješno pružaju institucijama, korporacijama i vladama širom svijeta, u Bosni i Hercegovini se u privatnom

[9] „Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace and Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU“
10 OECD definiše JPP kao „Aranžman u kojem privatni sektor nudi infrastrukturna dobra i usluge koja tradicionalno pružaju državne vlasti.“ https://stats.oecd.org/glossary/detail.asp?ID=7315
[11] https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models
[12] https://www.ecs-org.eu/documents/contract.pdf

sektoru razvija ovakva ekspertiza kroz globalna partnerstva i usluge, tipa davalac usluge upravljanja sigurnošću računarske mreže, MSSP (Managed Security Service Provider). Znanja, resursi i tehničke sposobnosti privatnog sektora mogu biti stavljeni na raspolaganje drugim javnim i privatnim organizacijama na permanentnoj osnovi ili kada se javi potreba, a posebno u kriznim situacijama.

Aktivnosti:

1. Ostvariti stratešku saradnju i uspostaviti kanale i okvire saradnje sa globalnim proizvođačima i ponuđačima proizvoda, rješenja i usluga iz domena cyber sigurnosti;
2. Uspostaviti direktnu saradnju i strateška partnerstva sa domaćim preduzećima koja nude proizvode, rješenja i usluge iz domena cyber sigurnosti s ciljem uspostavljanja odgovarajuće ekspertize, kadrovske baze i tehničkih resursa unutar Bosne i Hercegovine;
3. Uspostaviti takav vid direktne saradnje, javno-privatna partnerstva (JPP) sa ponuđačima, prije svega globalnim korporacijama iz sektora usluga cyber sigurnosti koji bi se mogli urgentno aktivirati u slučaju potrebe i kriznih situacija. Napraviti pregled ekspertskih znanja po operatorima ključnih usluga.

I2: Uspostavljeno javno-privatno partnerstvo sa operatorima ključnih usluga

Operatori ključnih usluga u privatnom vlasništvu podliježu obavezama zaštite svoje kritične informaciono-komunikacione infrastrukture u skladu sa uredbama regulatora i primjenljivom zakonskom regulativom pojedinačnih sektora. Ovim operatorima ne treba samo nametati obaveze već im pružiti i podršku u provođenju zaštite. Dobro organizovanom saradnjom moguće je racionalno koristiti ograničene ljudske resurse. Znanja i tehničke sposobnosti koje postoje u jednoj organizaciji, javnoj ili privatnoj, mogu biti stavljeni na raspolaganje drugim organizacijama iz tog sektora ili šire, kada se javi potreba, a posebno u kriznim situacijama.

Aktivnosti:

1. U saradnji sa nadležnim regulatornim tijelima precizno definisati obaveze privatnog sektora za osiguravanjem kritične informaciono-komunikacione infrastrukture, te osigurati odgovarajuće mehanizme kontrole;
2. Napraviti pregled ekspertskih znanja po operatorima ključnih usluga;
3. Podsticati uzajamnu stručnu podršku i razmjenu informacija među operatorima ključnih usluga unutar sektora, a po potrebi i šire.

I3: Uspostavljeno javno-privatno partnerstvo za razmjenu informacija

Razmjena informacija o cyber sigurnosno interesantnim događajima između svih organizacija, javnih i privatnih, omogućava pravovremeno i adekvatno reagovanje na njih. Potrebno je imati uspostavljene mehanizme razmjene i zaštite i tajnih podataka između domaćih i stranih privatnih kompanija i korporacija i javnog sektora u BiH. Potrebno je osigurati da sve uključene strane mogu aktivno učestvovati u razmjeni informacija u skladu sa zakonima.

Aktivnosti:

1. Privatna i javna preduzeća u skladu sa potrebama razmjene tajnih podataka će uspostavljati mehanizme razmjene i zaštite tajnih podataka kroz dobijanje industrijskih sigurnosnih dozvola (Facility Security Clearance) koje izdaje Državni sigurnosni organ (National Security Authority).

III. Zaključna razmatranja

Strateški okvir je početni korak u pravcu izgradnje sigurnijeg društva u cyber prostoru.

Ovaj dokument predstavlja smjernice za harmonizaciju postojećih i razvoj budućih strategija za sigurnost cyber prostora u BiH koji, kroz konkretne aktivnosti navedene u okviru opisa svakog od ciljeva, omogućava lakšu izradu strategija i akcionih planova. Akcionim planovima je potrebno definisati institucije odgovorne za provođenje aktivnosti u skladu sa nadležnostima, kao i rokove završetka, potrebne resurse i indikatore uspješnosti.

Uspješnost provođenja aktivnosti iz strateškog okvira kroz strategije i akcione planove zavisi od mnogih faktora. Na osnovu iskustava zemalja koje su prošle ovaj proces, ENISA[9] je prepoznala sljedeće najčešće izazove i otežavajuće okolnosti:

- **Uspostavljanje uspješne saradnje između institucija**
  Pitanje nadležnosti i odgovornosti za cyber sigurnost može biti teško za odgovoriti i riješiti. Ovo dovodi do rasipanja resursa za višestruku zaštitu od istog rizika ili potpunu nepokrivenost nekog rizika. Rješenje je u dobro uspostavljenoj strukturi i saradnji tijela zaduženih za osiguranje, jačanje i poboljšanje cyber sigurnosti.
- **Uspostavljanje povjerenja između javnog i privatnog sektora**
  Privatni sektor treba vjerovati da ulaganja u cyber sigurnost, pogotovo ako su nametnuta kroz propise, zapravo pomažu njegovom uspješnom poslovanju. Tada će privatni sektor prihvatiti ova ulaganja kao poslovnu potrebu, a ne nepotreban trošak. Javni sektor treba da vjeruje da novac uložen u povećanje sigurnosti privatnog sektora doprinosi sigurnosti cjelokupnog društva, a da nije suvišno izdvajanje iz budžeta.
- **Obezbjeđivanje odgovarajućih resursa**
  Da bi se ciljevi ostvarili potrebna su ulaganja. Kod cyber sigurnosti problemi često nisu materijalni, već su problemi ljudski resursi. Izgradnja potrebnog stručnog kadra je proces koji se ne može realizovati u kratkom vremenu i zato ovaj proces treba započeti odmah. Naravno, odgovarajući finansijski resursi su neophodni i za razvoj ljudskih potencijala i za nabavku opreme.
- **Promocija zajedničkog pristupa i podizanje svijesti o zaštiti podataka i privatnosti**
  Nedostatak zajedničkog pristupa svih učesnika zaštiti cyber sigurnosti dovodi do razjedinjenog i neefikasnog djelovanja. Potrebno je aktivno djelovati na podizanju svijesti, a posebno o tome da je potrebno usklađeno djelovanje. Pitanje privatnosti i zaštite podataka često se pojavi kao vrlo kompleksno za uravnotežen pristup.

- **Provedba analize sigurnosnih propusta i rizika**

  Ova analiza može biti vrlo zahtjevna i teška za provesti ako se zahtjevi postave preširoko. Preferira se fokusiran pristup na manje oblasti koji će rezultirati preciznijom i manje obimnom analizom rizika čiji rezultati se mogu direktno iskoristiti za provedbu konkretnih mjera.

Popularna fraza iz cyber sigurnosti kaže da je sigurnost proces, a ne proizvod ili stanje. Zbog toga ni strateški dokumenti nisu dokumenti koji se napišu jednom i koriste zauvijek. Strateške dokumente je potrebno redovno evaluirati u periodima ne dužim od iskazanog u viziji, što je u ovom slučaju pet godina. Evaluaciju treba da radi nezavisno tijelo od onog koje je pisalo ili provodi strateški okvir. Za evaluaciju je potrebno obezbijediti resurse. Evaluacijom se procjenjuje stepen ispunjenosti globalnih ciljeva, kao i realizacija i uspješnost pojedinih aktivnosti. Iz procesa provedbe strateškog okvira potrebno je uočiti dobre i loše prakse. Na osnovu rezultata evaluacije, kao i pregleda stanja cyber sigurnosti, radi se ažuriranje strateškog okvira. Ažuriranje uključuje izmjene globalnih ciljeva i pojedinih aktivnosti.

Da bi se olakšao i objektivizirao proces evaluacije potrebno je definisati ključne pokazatelje uspješnosti (Key Performance Indicators (KPI)) provedbe strateškog okvira. Za svaki od globalnih ciljeva, na osnovu planiranih aktivnosti, utvrđuju se konkretne i mjerljive veličine koje pokazuju u kojoj mjeri je planirana aktivnost ostvarena i koliko je doprinijela ostvarenju globalnog cilja.

- *Relevantni dokumenti korišteni u pripremi Smjernica su*:
  1. OSCE DECISION No. 1202 OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming From The Use of Information and Communication Technologies; PC.DEC/1202, od 10. marta 2016.; dostupno na: https://www.osce.org/pc/227281?download=true
  2. DIREKTIVA (EU) 2016/1148 EUROPSKOG PARLAMENTA I VIJEĆA o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (NIS direktiva)
  3. NCSS Good Practice Guide- Designing and Implementing National Cyber Security Strategies, 2016.
  4. Guide to Developing a National Cybersecurity Strategy, ITU, 2018.
  5. Konvencija o kibernetičkom kriminalu (Convention on Cybercrime, Budimpešta, 23.11.2001. godine, stupila na snagu 01.07.2004. godine, stupila na snagu u odnosu na BiH 01.09.2006. g; objava „Službeni glasnik BiH"– Međunarodni ugovori broj: 06/2006);
  6. Dodatni protokol uz Konvenciju o kibernetičkom kriminalu, o inkriminiranju djela rasističke i ksenofobne naravi počinjenih pomoću računarskih sistema (Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, Strasbourg, 28.01.2003. godine, stupio na snagu 01.03.2006. g, stupio na snagu u odnosu na BiH 01.09.2006. godine; objava „Službeni glasnik BiH" - Međunarodni ugovori broj: 06/2006);

7. Izvještaj o rezultatima godišnje ankete korisnika RAK dozvola za pružanje Internet usluga u Bosni i Hercegovini za 2018. godinu - procjenjuje se da je u 2018. godini bilo 3,195,294 korisnika Interneta, odnosno da stopa korištenosti Interneta u Bosni i Hercegovini za 2018. godinu iznosi 90,49%. Dostupno na: https://docs.rak.ba//documents/ea9d822c-b1dc-4ad9-b2d9-735dc6c8ea91.pdf
8. (hrv.) UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka); Dostupno na: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1552662547490&uri=CELEX%3A32016R0679.
9. CYBERSECURITY CAPACITY REVIEW, Bosnia and Herzegovina, Global Cyber Security Capacity Centre, mart 2019.
10. Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace, OSCE, 2013.
11. Strategija cyber sigurnosti - uspostava sistema za osiguranje visokog stepena cyber sigurnosti u Ministarstvu odbrane i Oružanim snagama Bosne i Hercegovine, 2017.
12. Developing a National Strategy for Cybersecurity - Foundations For Security, Growth, and Innovation, Microsoft, 2013.
13. National strategy for the protection of Switzerland against cyber risks, 2012.
14. Finland´s Cyber security Strategy, 2013.
15. National Cyber Security Strategy, Spain, 2013.
16. Odluka o donošenju nacionalne strategije kibernetičke sigurnosti i akcijskog plana za provedbu nacionalne strategije kibernetičke sigurnosti, Hrvatska, 2015.
17. Strategija razvoja informacione bezbednosti u Republici Srbiji za period od 2017. do 2020. godine, 2017.
18. Strategija sajber bezbjednosti Crne Gore 2018-2021, 2017.
19. National Cyber Security Strategy 2016-2021, UK, 2016.
20. National Cyber Security Strategy 2, From awareness to capability, Netherlands, 2018.
21. A national cyber security strategy, Sweden, 2017.
22. National Cyber Security Strategy, of the United States of America, 2018.

PRILOG I - OBAVEZNI SEKTORI KLJUČNIH USLUGA PREMA NIS DIREKTIVI

1. Energetika
    a. električna energija
    b. nafta
    c. plin
2. Prevoz
    d. vazdušni
    e. željeznički
    f. vodeni
    g. cestovni
3. Bankarstvo
4. Infrastruktura finansijskog tržišta
5. Zdravstvo
6. Vodosnabdijevanje
7. Digitalna infrastruktura

Obavezne digitalne usluge (NIS direktiva prilog III)

1. Internetsko tržište
2. Internet pretraživač
3. *Cloud computing* usluge

PRILOG II - OPERATORI KLJUČNIH USLUGA PREMA NIS DIREKTIVI

1. **Energetika**
   a. Električna energija
      - Elektroenergetska preduzeća koja obavljaju najmanje jednu od sljedećih funkcija: proizvodnja, prenos, distribucija, snabdijevanje ili nabavka električne energije, i koja su odgovorna za komercijalne, tehničke ili zadatke održavanja povezane sa tim funkcijama
      - Operatori prenosnog i distribucijskog sistema električne energije

   b. Nafta
      - Operatori naftovoda
      - Operatori proizvodnje nafte, rafinerija i tvornicâ nafte te njezina skladištenja i prenosa

   c. Plin
      - Preduzeća za opskrbu plinom
      - Operatori distribucijskog sistema plina
      - Operatori transportnog sistema plina
      - Operatori sistema skladišta plina
      - Operatori terminala za ukapljeni prirodni plin
      - Preduzeća za prirodni plin
      - Operatori postrojenja za rafiniranje i obradu prirodnog plina

2. **Prevoz**
   a. Vazdušni
      - Vazdušni prevoznici
      - Upravno tijelo aerodroma i aerodrom, te tijela koja upravljaju pomoćnim objektima u aerodromima
      - Operatori kontrole upravljanja saobraćajem koji pružaju usluge kontrole vazdušnog saobraćaja

   b. Željeznički
      - Upravitelji željezničke infrastrukture
      - Željeznički prevoznici, među ostalim i operatori uslužnih objekata

   c. Vodeni
   - Kompanije za prevoz putnika unutarnjim plovnim putevima, morem i duž obale te kompanije za prevoz tereta unutarnjim plovnim putevima, morem i duž obale, ne uključujući pojedinačna plovila kojima upravljaju te kompanije
   - Upravljačka tijela luka, uključujući njihove luke, te subjekti koji upravljaju postrojenjima i opremom u lukama
   - Služba za nadzor i upravljanje pomorskim saobraćajem

   d. Cestovni
      - Tijela nadležna za ceste odgovorna za upravljanje saobraćajem
      - Operatori inteligentnih saobraćajnih sistema

3. **Bankarstvo**
      - Kreditne institucije

4. **Infrastruktura finansijskog tržišta**
      - Operatori mjesta trgovanja
      - Središnje druge ugovorne strane (tekst preuzet iz 648/2012. član 2. stav 1.)

5. **Zdravstvo**
      - Davaoci zdravstvene zaštite

6. **Vodosnabdijevanje**
      - Dobavljači i distributeri vode namijenjene za ljudsku potrošnju, ali isključujući distributere kojima distribucija vode za ljudsku potrošnju čini samo dio njihove opšte aktivnosti distribucije druge robe i proizvoda koji se ne smatraju ključnim uslugama

7. **Digitalna infrastruktura**
      - IXP-ovi
      - Davaoci DNS usluga
      - Registri naziva TLD-ova

PRILOG III - ZAHTJEVI U POGLEDU TIMOVA ZA ODGOVOR NA RAČUNARSKE SIGURNOSNE INCIDENTE (CSIRT-ovi) I NJIHOVI ZADACI PREMA NIS DIREKTIVI

1. Zahtjevi u pogledu CSIRT-ova:

    a. CSIRT-ovi osiguravaju visok nivo dostupnosti svojih komunikacijskih usluga izbjegavanjem jedinstvenih tačaka prekida te u svakom trenutku raspolažu s nekoliko sredstava za mogućnost dvosmjernog kontaktiranja. Nadalje, komunikacijski kanali jasno su određeni i dobro poznati klijentima i saradnicima.
    b. Prostori CSIRT-ova i informacioni sistemi za podršku smješteni su na sigurnim lokacijama.
    c. Kontinuitet rada:
        i. CSIRT-ovi su opremljeni odgovarajućim sistemom za upravljanje zahtjevima i njihovim preusmjeravanjem, kako bi se olakšale primopredaje.
        ii. CSIRT-ovi imaju dovoljno kvalifikovanih zaposlenika kako bi se osigurala dostupnost u svako doba.
        iii. CSIRT-ovi se oslanjaju na infrastrukturu čiji je kontinuitet osiguran. U tu svrhu dostupni su redundantni sistemi i rezervni radni prostor.
    d. CSIRT-ovi imaju mogućnost da, ako to žele, učestvuju u međunarodnim mrežama za saradnju.

2. Zadaci CSIRT-ova:

    a. Zadaci CSIRT-ova obuhvataju barem:
        i. praćenje incidenata;
        ii. pružanje ranih upozorenja i najava te informisanje relevantnih učesnika o rizicima i incidentima;
        iii. odgovaranje na incidente;
        iv. pružanje dinamičke analize rizika i incidenata te pregleda situacije;
        v. učestvovanje u mreži CSIRT-ova.
    b. CSIRT-ovi uspostavljaju saradnju s privatnim sektorom.
    c. CSIRT-ovi s ciljem olakšavanja saradnje promovišu usvajanje i primjenu zajedničkih ili normiranih praksi za:
        i. postupke rješavanja incidenata i rizika;
        ii. planove za klasifikaciju incidenata, rizika i informacija.

PRILOG IV - DEFINICIJE i SKRAĆENICE

CERT (*Computer Emergency Response Team*) - tim za odgovor na računarsku opasnost

Cloud computing - digitalna usluga kojom se pruža pristup nadogradivom i elastičnom skupu djeljivih računarskih resursa.

CSIRT (*Computer Security Incident Response Team*) - tim za odgovor na računarske sigurnosne incidente

Cyber - odnosi se na ljude, stvari, politike, pojmove i ideje povezane sa računarskim uređajima i računarskim mrežama, a posebno Internetom i informacionim tehnologijama.

Cyber kriminal - kriminalne aktivnosti u kojima su informaciono-komunikacioni sistemi predmet, sredstvo, cilj ili mjesto krivičnog djela.

Cyber prostor - više nego Internet, uključuje ne samo hardver, softver i informacione sisteme, već i ljude i društvenu interakciju u okviru ovih mreža.

Davalac DNS usluge - subjekt koji pruža DNS (Domain Name System - Sistem naziva domena) usluge na Internetu

DNS (*Domain Name System*) - Sistem naziva domena

ENISA (*European Network and Information Security Agency*) - Agencija Evropske unije za mrežnu i informacionu sigurnost

EU – Evropska unija

Facility Security Clearance –dobijanje industrijskih sigurnosnih dozvola

FIRST (*Forum for Incident Response and Security Teams*) – forum za timove za sigurnost i odgovor na incidente

GDPR – (*General Data Protection Regulation*) UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA i VIJEĆA o zaštiti pojedinaca u vezi s obradom ličnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opšta uredba o zaštiti podataka)

GEANT – pan-evropska računarska mreža za istraživačku i obrazovnu zajednicu

IKT – informaciono-komunikacione tehnologije

Incident - bilo koji događaj koji ima stvaran negativni učinak na sigurnost informaciono-komunikacionih sistema;

Informaciono-komunikacioni sistem

a. bilo koji uređaj ili grupa povezanih ili srodnih uređaja, od kojih jedan ili više njih programski izvršava automatsku obradu digitalnih podataka;
b. digitalni podaci koji se pohranjuju, obrađuju, dobivaju ili prenose elementima opisanim u „a.“ u svrhu njihova rada, upotrebe, zaštite i održavanja;

Informaciona sigurnost - stanje povjerljivosti, cjelovitosti i dostupnosti informacija

Internet pretraživač - digitalna usluga koja korisniku omogućava da vrši pretraživanja u načelu svih internetskih stranica ili internetskih stranica na određenom jeziku na osnovu upita, o bilo kojoj temi, koji

je u obliku ključne riječi, rečenice ili nekog drugog unosa, a rezultat su *link*-ovi na kojima se mogu pronaći informacije koje su povezane sa zatraženim sadržajem;

Internetsko tržište - digitalna usluga koja potrošačima i/ili trgovcima, omogućava da na Internetu sklapaju kupoprodajne ugovore i ugovore o uslugama s trgovcima na web stranici tog internetskog tržišta ili na web stranici tog trgovca koji se služi računarskim uslugama koje pruža internetsko tržište;

ISO (*International Organization for Standardization*) – Međunarodna organizacija za standardizaciju

ISP (*Internet Service Provider*) – davalac usluge pristupa internetu

ITU (*International Telecommunication Union*) – Međunarodna telekomunikaciona unija

IXP (*Internet eXchange Point*) - neutralna tačka za razmjenu internetskog saobraćaja

JPP- Javno- privatno partnerstvo

Ključna usluga - usluga koja je ključna za održavanje ključnih društvenih i/ili ekonomskih djelatnosti, a minimalno usluge definisane u Prilogu I

KPI (*Key Performance Indicator*) – ključni pokazatelj uspješnosti

Kritična informaciono-komunikaciona infrastruktura – informaciono-komunikaciona infrastruktura operatora ključne usluge neophodna za pružanje te ključne usluge

Krizna situacija - situacija u kojoj je ugroženo funkcionisanje kritične informaciono-komunikacione infrastrukture, a time i pružanje ključnih usluga;

MSSP-(*Managed Security Service Provider*)- davalac usluge upravljanja sigurnošću računarske mreže

Neutralna tačka za razmjenu internetskog saobraćaja (IXP) - mrežni instrument koji omogućava međusobno povezivanje dva ili više nezavisnih autonomnih sistema, prvenstveno u svrhu olakšavanja razmjene internetskog saobraćaja; IXP pruža međusobno povezivanje samo za autonomne sisteme;

NIS direktiva – (Network and Information Security) DIREKTIVA (EU) 2016/1148 EUROPSKOG PARLAMENTA I VIJEĆA o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sistema širom Unije

NIST (*National Institute of Standards and Technology*) – Institut za standarde i tehnologiju SAD

Operator ključne usluge - javni ili privatni subjekt tipa navedenog u Prilogu II koji pruža neku od ključnih usluga

OSCE – Organizacija za sigurnost i saradnju u Evropi

Registar naziva vrhovnih domena - subjekt koji upravlja i rukuje registracijom naziva internetskih domena za određenu vrhovnu domenu (TLD);

Rizik - bilo koja razumno prepoznatljiva okolnost ili događaj koji ima potencijalan negativni učinak na sigurnost informaciono-komunikacionih sistema;

Sigurnost informaciono-komunikacionih sistema - sposobnost informaciono-komunikacionih sistema da odolijevaju, na određenoj razini pouzdanosti, bilo kojoj radnji koja ugrožava dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih ili prenesenih ili obrađenih podataka ili srodnih usluga koje ti informaciono-komunikacioni sistemi nude ili kojima omogućavaju pristup;
Sistem naziva domena (vidjeti DNS Domain Name System) - hijerarhijsko raspoređeni sistem imenovanja na mreži koji daje odgovore na upite o nazivima domena;

TLD (*Top-level Domain*) **-** vrhovna domena

TF-CSIRT (*Task Force Computer Security Incident Response Teams*) – GEANT radna grupa za CSIRT-ove

UN – Ujedinjene nacije

PRILOG V - GENERALNI PREGLED POSTOJEĆIH MEĐUNARODNIH OBAVEZA, POLITIKA, STRATEGIJA, ZAKONA I PROPISA KOJI SE U ODNOSE NA CYBER SIGURNOST U BOSNI I HERCEGOVINI

Međunarodne obaveze:

Niz rezolucija Generalne skupštine UN-a koje se odnose na cyber sigurnost

OSCE-ove Mjere izgradnje povjerenja kako bi se smanjili rizici od sukoba koji proizlaze iz korištenja IKT-a

Strategija cyber sigurnosti Evropske unije

DIREKTIVA (EU) 2016/1148 EUROPSKOG PARLAMENTA I VIJEĆA o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (NIS direktiva)

Konvencija Vijeća Evrope o cyber kriminalu / Budimpeštanska konvencija

Međunarodni propisi o telekomunikacijama

EU (Komisija) Digitalna agenda za Zapadni Balkan

Pakt stabilnosti – inicijativa za elektronsku jugoistočnu Evropu –

Politike:

Politika razvoja informacionog društva za razdoblje 2017.-2021. godina (veza strana 19. III stub - Potjecanje povjerenja i sigurnosti) („Službeni glasnik BiH broj 42/17) Bosne i Hercegovine

Strategije:

Strateški plan Ministarstva sigurnosti Bosne i Hercegovine za period 2017-2019,

Strategija za borbu protiv terorizma za period 2015.-2020. u Bosni i Hercegovini

Strategija za borbu protiv organizovanog kriminala za period 2017.-2020. u Bosni i Hercegovini

Akcioni plan za zaštitu djece i sprečavanje nasilja nad djecom počinjeno putem IKT-a u Bosni i Hercegovini

Strategija cyber sigurnosti Ministarstva odbrane Bosne i Hercegovine

Akcioni plan Ministarstva odbrane BiH o cyber sigurnosti

Zakoni:

Zakon o informacionoj bezbjednosti Republike Srpske ("Službeni glasnik RS" broj 70/11)

Zakon o bezbjednosti kritičnih infrastruktura Republike Srpske ("Službeni glasnik RS" broj 58/19)

PRILOG VI - INSTITUCIJE, TIJELA I POSMATRAČI, ČLANOVI NEFORMALNE RADNE GRUPE KOJI SU DOPRINIJELI IZRADI SMJERNICA ZA STRATEŠKI OKVIR CYBER SIGURNOSTI U BOSNI I HERCEGOVINI POD OKRILJEM MISIJE OSCE-A U BOSNI I HERCEGOVINI

Posmatrači
Međunarodne organizacije i diplomatske misije
1. G. Mak Kamenica, Aktivnosti ulaganja u energetiku, zamjenik direktora USAID;
2. G. Milan Sekuloski, viši savjetnik za područje Evrope i Centralne Azije, DCAF - Geneva Centre for Security Sector Governance;
3. Gđa. Irina Rizmal, DCAF – asistentica na projektu za područje Evrope i Centralne Azije, DCAF - Geneva Centre for Security Sector Governance;
4. G. Adel Abusara, viši asistent projekta, Demokratsko upravljanje, Misija OSCE-a u Srbiji;

Akademska zajednica:
1. G. Saša Mrdović, profesor, Odsjek za računarstvo i informatiku, Elektrotehnički fakultet, Univerzitet Sarajevo;
2. G. Emir Vajzović, docent, Rukovodilac Instituta za društvena istraživanja; Fakultet političkih nauka, Univerzitet u Sarajevu;

Vijeće ministara Bosne i Hercegovine
3. Gđa. Ivana Šarić, šefica Službe za održavanje i razvoj sistema elektronskog poslovanja i e- Vlade, Generalni sekretarijat Vijeća ministara BiH;
4. G. Ivan Brčić, viši stručni saradnik, Služba za održavanje i razvoj sistema elektronskog poslovanja i e-Vlade, Generalni sekretarijat Vijeća ministara;

Ministarstvo odbrane Bosne i Hercegovine
5. G. Belmir Agić, pomoćnik ministra, Sektor K4UI, Ministarstvo odbrane BiH;

Ministarstvo vanjskih poslova BiH
6. Gđa. Stela Šunjić, ministar-savjetnik, šefica Odsjeka za komunikacije i informatiku;
7. G. Mirza Pašić, stručni savjetnik, Odjel za OSCE, VE i Regionalne inicijative;

Ministarstvo sigurnosti BiH
8. G. Mate Miletić, pomoćnik ministra, Sektor zaštite tajnih podataka;
9. G. Adnan Kulovac, šef Odsjeka za informatičku sigurnost;
10. G. Mustafa Arifović, stručni savjetnik za IT, Direkcija za koordinaciju policijskih tijela;
11. G. Željko Dugonjić, stručni savjetnik;

Ministarstvo komunikacija i transporta BiH
12. G. Branislav Zimonjić, viši stručni saradnik za IT;
13. Gđa. Irida Varatanović, savjetnica ministra;
14. G. Damir Prlja, MAP REA kontakt osoba za BiH u oblasti Digitalnih integracija;

Državna agencija za istrage i zaštitu (SIPA)
15. G. Alis Gabeljić, istražitelj, Kriminalističko-istražni odjel, Državna agencija za istrage i zaštitu;

Obavještajno-sigurnosna agencija
16. G. Nermin Mehić, šef odjela, Obavještajno-sigurnosna agencija;

Ministarstvo vanjske trgovine i ekonomskih odnosa Bosne i Hercegovine:
17. Gđa. Vera Vitomir, Odjel za energetski sektor;

Energetski sektor

18. G. Edin Zametica, sekretar, Državna regulatorna komisija za električnu energiju (DERK);
19. Gđa. Amra Omeragić, savjetnica generalnog direktora, Elektroprenos Bosne i Hercegovine;
20. G. Darko Sinanović, rukovodilac Službe za informacione i telekomunikacijske sisteme; Nezavisni operator sistema u Bosni i Hercegovini (NOS BiH);
21. Gđa. Emina Kreštalica, inžinjer za razvoj softvera, JP Elektroprivreda BiH d.d. Sarajevo;
22. G. Jasmin Heljić, inžinjer za razvoj softvera, JP Elektroprivreda BiH d.d. Sarajevo;

Regulatorna agencija za komunikacije BiH

23. G. Aleksandar Mastilović, stručni savjetnik generalnog direktora;
24. G. Predrag Divljan, šef IT odjela;

Privatni sektor

25. G. Enes Haračić, direktor, Results Consulting;

Vlada Federacije Bosne i Hercegovine

26. G. Adi Kantardžić, stručni saradnik, IT Sektor, Generalni sekretarijat Vlade Federacije BiH;
27. G. Adis Omerović, član radne grupe na ICIS Projektu;

Ministarstvo unutrašnjih poslova Republike Srpske

28. G. Dragan Grmuša, načelnik Odjeljenja za strateško planiranje, Služba ministra;
29. Gđa. Divna Lovrić, načelnica Uprave za IKT;
30. Dr Gojko Pavlović, Odjeljenje za međunarodnu saradnju, Služba ministra;
31. G. Olivije Zimonja, načelnik Odjeljenja za visoko-tehnološki kriminalitet, Uprava kriminalističke policije;

Ministarstvo za naučnotehnološki razvoj, visoko obrazovanje i informaciono društvo Republike Srpske

32. G. Aleksandar Đurić, CERT Republike Srpske;

Ministarstvo unutrašnjih poslova Federacije BiH

33. G. Nedžad Ćatić, šef Odsjeka za borbu protiv kompjuterskog kriminala;
34. G. Saša Petrović, inspektor, Federalna istražna služba kriminalističke policije;

Policija Brčko distrikta BiH

35. G. Neđo Lazarević, istražitelj u Jedinici kriminalističke policije;

Delegacija Evropske unije u BiH i Specijalni predstavnik Evropske unije u BiH

36. G. Šadi Matar, politički savjetnik, Informaciono društvo i mediji;

Misija OSCE-a u Bosni i Hercegovini

37. G. Bojan Janković, koordinator programa Odjel za sigurnosnu saradnju;
38. Gđa. Sanja Ćatibović, službenik Odjela za sigurnosnu saradnju, (kontakt osoba za pitanja cyber sigurnosti)