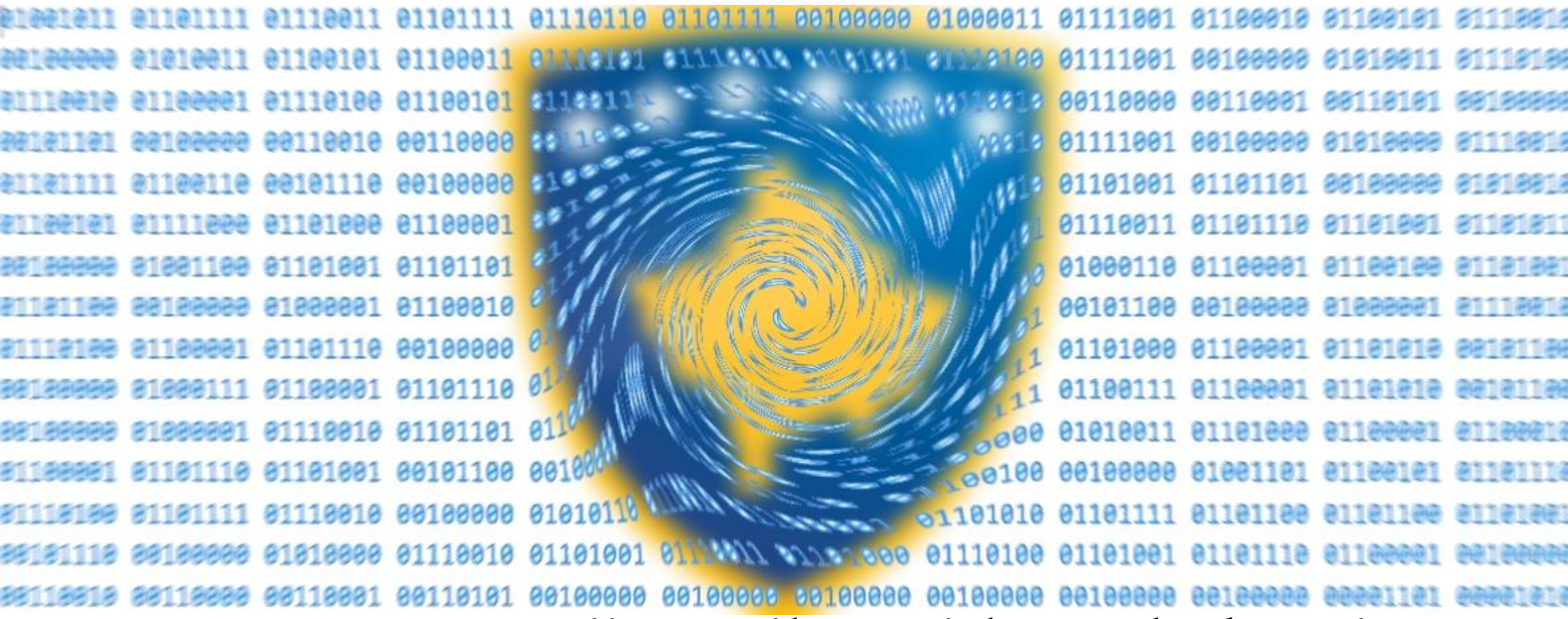
REPUBLIKA E KOSOVËS
REPUBLIKA KOSOVA / REPUBLIC OF KOSOVO

QEVERIA E KOSOVËS
VLADA KOSOVA / GOVERNMENT OF KOSOVO

MINISTRIA E PUNËVE TË BRENDSHME
MINISTARSTVO UNUTRAŠNJIH POSLOVA
MINISTRY OF INTERNAL AFFAIRS



Državna Strategija za Kiberneticku Bezbednost i Akcioni Plan 2016 – 2019

Decembar 2015

Izvršni zbir

Internet danasnjice sa kibernetickim prostorom (virtuelnom) je najveći sistem koji je ikada stvoren od čovečanstvo, sa milijardama uređaja koji su povezani kroz više komunikacionih veza, sa milijardama korisnika povezanim sa laptopovima, tabletima i pametnim telefonima. Trend je da svaki I sve sto se moze povezati, a taj trend ima tendenciju da ide u pravcu daljeg rasta. Prema Svetskim Statistikama Interneta (World Internet Statistic) povećana upotreba interneta za period 2000. do 2014. godine bio je 741 %, dok je Internet penetracija na globalnom nivou iznosi oko 42 %. Iako , prema Gartner, Inc. , 2020. biće oko 26 milijardi uređaja na Internetu. Sa ovim velikim korišćenjem Interneta kao glavni radna platforma, komunikacije nauke i savremenenog društvenog građanina, nejgova bezbednost i privatnost se vracaju na glavnu brigu.

Internet se njegovim kibernetickim prostorom predstavlja jedan od najvažnijih pokretača inovacija, rasta i konkurentnosti nacionalnih ekonomija u svetu. U globalizovanom i povezanom kibernetickom prostoru i njegovoj bezbednosti se vracaju kao ključni strateški ciljevi u oblasti bezbednosti u svakoj zemlji. Internet I njegove kiberneticke aktivnosti, kao što su ekonomski, naučni i društveni, dobijaju veću važnost svaki dan. Ova kibernetska sloboda i ljudskih vrednosti moraju biti zaštićene na isti način kao u svetu van interneta. Digitalna infrastrukturu treba da bude zaštićeni od potencijalnih incidenata, zloupotrebe i zlonamerne aktivnosti. Javne institucije Kosova treba da imaju glavnu ulogu, prvobitno uspostavljajuci jasnu politiku i transparentne smernice kako bi se osiguralo da samo otvaranje i učešće svakog građanina, već i sigurnost kibernetickog prostora.

Na Kosovu, upotreba informacionih i komunikacionih tehnologija (IKT) se brzo proširila od 2000. godine, dok IKT je već igra važnu ulogu u svim aspektima našeg života. Internet penetracija na Kosovu je 76,6%, ovaj stepen je vrlo slična sa prosekom Evropske Unije (EU), dok i ponašanje Kosovara u internetu izgleda slično sa globalnim trendovima. Vecina kosovskih institucija us pomerili svoje svakodnevne zadatke na mreži, uključujući i organizacije koje pružaju usluge u kritičnim infrastrukturnim sektorima kao što su energija, voda, zdravstvo, transport, komunikacije i vladinih i drugih organizacija. Ovi sistemi poboljšavaju kvalitet i brzinu usluga koje se pruzaju, pomažući tako organizacijama za više produktivan rad, doprinoseći poboljšanju životnog standarda. Međutim, u isto vreme, oni su izloženi različitim rizicima u prostoru interneta. Ovi rizici stoje kod neizbežno IKT, i mogu izazvati nedostatak usluga ili zloupotrebe usluga, što dovodi do oštećenja (gubitak) potencijalnihg ljudskih života, ekonomske gubitke u velikoj meri, uništenje javnog reda, pretnje po nacionalnu bezbednost.

U tom kontekstu, Vlada Republike Kosova je uključila u Program Vlade 2015-2018 izradu Nacionalne Strategije Kiberneticke Bezbednosti 2016 - 2019 i Akcionog plana, kao i Odluke br. 30/01 od 05.20.2015 uključeni u strategiju planskih dokumenata za 2015. Radna grupa sa svim uključenim stranama je osnovana u okviru Ministarstva Unutrašnjih Poslova (MUP) . Radna grupa ima mandat da pripremi politike, strategije i akcioni plan za kiberneticku bezbednost na državnom nivou. Sve organizacije, I drzavne agencije, fizičkih i pravnih lica dužni su da obavljaju poslove utvrđene u okviru politika, strategija i akcionih planova postavljenih od strane Saveta Kibernticke Bezbednosti.

Nacionalna Strategija za Kiberneticku Bezbednost se bavi pitanjem kiberneticke bezbednosti na Kosovu kroz ove strateške ciljeve :

1. Zaštita kritične strukture informacije;
2. Institucionalni razvoj i jačanje kapaciteta;
3. Izgrdanja javno-privatnih partnerstva;
4. reagovanje prema incidentima;
5. Međunarodna saradnja;

Sadržaj

Lista skracenica

KI	Kriticna Infrastruktura
KII	Kriticna Infrastruktura Informacije
ZKII	Zastita Kriticne Infrastrukture Informacije
VK	Vlada Kosova
ERKE	Ekipa Reagovanja za Kompjuterske Emergence
ERIKB	Ekipa Reagovanja za Kompjuterske Bezbednosti
EABIM	Evropska Agencija za Bezbednost Informacionih Mreza
TIK	Tehnologija Informisanja i Komuniciranja
MUP	Ministarstvo Unutrasnjih Poslova
NATO	Organizata Severno-Atlantskog Traktata
NSKB	Drzavni savet za Kiberneticku Bezbednost
OSER	Organizacijza za Saradnju I Ekonomski Razvoj
OSBE	Organizacija za Saradnju i Bezbednost u Evropi

1 Uvod

1.1 Svrha dokumenta

Svrha ovog dokumenta je da se uspostavi osnovu Nacionalne Strategije za kiberneticku bezbednost za naredne tri godine u Republici Kosovo. Štaviše, ovaj dokument definiše viziju Vlade Kosova za kiberneticku bezbednost i relevantnog akcionog plana. Nacionalna Strategija za kiberneticku bezbednost je deo Programa Vlade 2015-2018 i povezano sa Nacionalnim Planom za adaptiranje Asquisa.

U ovom dobu globalizacije, nakon energije, kiberneticka bezbednost je postala jedan od glavnih strateških ciljeva svake zemlje. Digitalna revolucija je dodirnula svaku sferu života u savremenom svetu. Više nego ikada, svaka zemlja pokušava da iskoristi kiberneticki prostor gurajuci napred ekonomski, naučnih i socijalni, ali i politički razvoj. Razvoj digitalne infrastrukture, kao Internet je promenio naš svakodnevni život socijalni i ekonomski. Sama promena mentaliteta ka digitalnoj infrastrukture se dešava.

Sloboda Internet i ljudske vrednosti moraju biti zaštićeni na isti način kao I van Interneta. Digitalna infrastruktura treba da bitit zaštićena od potencijalnih incidenata i zlonamernih radnji. Javne institucije imaju veliku ulogu, prvobitno postavljenje smernica i jasnih politike i transparentne, da bi ne samo otvaranje i učešće svakog građanina, već i sigurnost u kibernetickom prostoru.

U 2013, Kosovsko Udruženje Informacione i Komunikacione tehnologije (STIKK) objavio je studiju o internet penetracije i korišćenja na Kosovu[1]. Prema ovoj studiji, penetracija interneta na osnovu domaćinstava je 84,8%, dok je prema korisnicima je 76,6 % , što je veoma blizu proseka Evropske Unije (EU) . Osim toga, studija navodi da se ponašanje većine Kosovara u internetu može porediti sa globalnim trendovima.

Pozivajući se na "*Analizu strateškog pregleda sektora bezbednosti na Kosovu*[2]" nekonvencionalni kiberneticki kriminal kao zločin je identifikovan kao jedan od rizika, izazova i globalnih pretnji koje mogu uticati na bezbednost Kosova.

Republika Kosovo je posvećena promovisanju stabilnosti i bezbednosti, ne samo u zemlji, već takođe biti značajan doprinos bezbednosti u regionu i šire. Dakle, međunarodna saradnja u oblasti kiberneticke bezbednosti ostaje prioritet za Kosovo.

1.2 Vizija

Kosovo će obezbediti bezbedno okruženje za kiberneticki prostor, minimiziranje i sprečavanje kiberneticke pretnje, u saradnji sa lokalnim i međunarodnim partnerima.

[1] http://www.stikk-ks.org/uploads/downloads/Internet_penetration_and_usage_in_Kosovo.pdf
[2] http://www.kryeministri-ks.net/repository/docs/Analysis_of_Strategic_Security_Sector_Review_of_RKS_060314.pdf

1.3 Definisanje izraza

Na Evropski i međunarodnim nivoima, ne postoji usklađena definicija ono što se zove "kibernetika" i "kiberneticka bezbednost". Značenje kiberneticke bezbednosti i drugih važnih uslova varira od zemlje do zemlje.

U ovom poglavlju, definicije posebnih termina javljaju usklađeni sa osnovnim značenjem ovih pojmova u zemljama EU. Svrha ove liste je da se podigne svest o opštoj populaciji u kompjuterskoj terminologiji.

"**Kibernetika**" (cyber) se definiše kao "*sve što ima veze sa, ili uključujući računare ili računarske mreže (poput interneta)*".

Prema Međunarodnoj Organizaciji za standardizaciju (ISO), "Cyber" je " kompleksna sredina koja proizilazi iz interakcije ljudi, programa i usluga na Internetu, pomoću opreme umrežavanja tehnologije u vezi sa njima, što ne postoji u fizičkom obliku".

Kiberneticki prostori

Kiberneticki prostor je virtuelni prostor svih IT sistema povezanih na podacima na globalnom nivou. Osnova kibernetickog proctor je Internet kao univerzalnA mrežA javno dostupnih i saobraćajnim vezama, koje mogu biti dopunjene i dalje proširiti na bilo koji broj drugih mreža podataka. IT sistemi u virtuelnim prostorima izolacije nisu deo kibernetickog prostora.

Takođe, poznato je da je globalno okruženje je stvorena kroz povezivanje informacionih i komunikacionih sistema. Kiberneticki prostor uključuje fizičke i virtuelne računarske mreže, računarskih sistema, formata i digitalnih podataka.

Kiberneticka bezbednost

U Strategiju Kiberneticke Bezbednosti Evropske Unije (Otvreni kiberneticki prostor, siguran i zaštićen[3])", *kiberneticka bezbednost uglavnom odnosi se na zaštitne mere i radnje koje se mogu preduzeti radi zaštite kibernetickog domena, čak iu civilnom i vojnom, od upozorenja u vezi sa njima ili da mogu narušiti komunikacione mreže i zavisne infrastrukture. Kiberneticka bezbednost nastoji da održi dostupnost i integritet mreže i infrastrukture, kao i poverljivost informacija koje u njima održavaju*".

Međunarodna Organizacija za Standardizaciju (ISO) definiše kiberenticki bezbednost kao " *očuvanje poverljivosti, integriteta i dostupnosti informacija u kibernetickom prostoru*".

Ostale definicije definišu kiberneticku bezbednost kao željeni cilj bezbednost IT, u kojem su rizici od globalnog kibernetickog prostora se sužavaju na prihvatljiv minimum. Dakle, kiberneticka bezbednost na Kosovu je željeni cilj za IT, u kojoj će se opasnosti kibernetickog prostora Kosova biti svedena na prihvataljiv minimum. Kiberneticka bezbednost (na Kosovu) je odgovarajuća i adekvatna količina. Kiberneticka bezbednos se fokusira na svim IT sistemima za civilnu upotrebu u kibernetickom prosstoru Kosova. Takođe je poželjno stanje u kome je zaštita kibernetickog prostora je proporcionalan kibernetickom pretnjama i mogućim posledicama kibernetickih napada.

Kiberneticki kriminal

Prema navedenoj strategiji za kiberneticku bezbednost Evropske Unije, "Kiberneticki kriminal generalno se odnosi na širok spektar kriminalnih aktivnosti, gde su računari i informacioni sistemi

[3]JOIN(2013) 1 final, 7 Feb 2013 - http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013JC0001

se anagzuju kao primarno sredstvo ili kao primarna meta. Kiberneticki kriminal obuhvata tradicionalna dela (npr prevara, falsifikovanje i kršenje identiteta), radi o sadržaju (npr Internet distribuciju pornografije dece ili izazivanje rasne mržnje) i radove koji su jedinstveni za računare i informacioni sistemi (npr napadi informacionih sistema, uskraćivanja usluga i malvare (maleare)".

On se sastoji se od krivična dela počinjena u mrežama, preko elektronskih komunikacionih mreža i informacija. Problem je neograničen, koji se mogu svrstati u tri definicije i šire[4]:
• I specifična krivična dela nterneta, - kao što su napadi na informacione sisteme ili phishing (npr lažne stranice banaka da se uzmu lozinke koje omogućavaju pristup bankovnim računima žrtava).
• Prevare i kiberneticka falsifikovanja, krađa identiteta, phishing, neželjene pošte, kloniranje kreditnih kartica i drugih kartica, i zlonamerano kodiranje.
• Nelegalni sadržaj online, uključujući i materijal sa seksualnom zlostavljanju dece, mržnje, podsticanje na terorističke akte i idealizma nasilja, terorizma, rasizma i ksenofobije.

Kiberneticki napadi, kiberneticko spijuniranje o kiberneticka sabotaza
Kiberneticki napad je napad na IT kibernetickom prostoru, usmeren protiv jednog ili više tehnoloških sistema u cilju kršnja sigurnosti IT. Ciljevi bezbednosti, poverljivosti, integriteta i dostupnosti to može biti ugrožena, pojedinačno ili u grupama. Kiberneticki napadi na poverljivost IT sistema, koje obavljaju ili upravljaju strane obaveštajne službe nazivaju kiberneticka špijunaža. Kiberneticki napadi protiv integriteta i dostupnosti IT sistema nazivaju se kiberneticka sabotaža.

Kiberneticka zastita - uglavnom se koristi u vojnom kontekstu, ali može imati veze sa kriminalnim aktivnostima i špijuniranjem. NATO koristi ovu definiciju da objasni sposobnost za odbranu od kibernetickog napada " spoosbnost za zaštitu i pruzanje upravljanja sa Sluzbama Informacionih Sistema (SKI) kao odgovor na moguće akcije, bliskih ali i nastalih zlonamerne koje se pojavljuju u kibernetickom prostoru". Kiberneticka zaštita se sastoji od sledećih zadataka: zaštita, otkrivanje, odgovor i oporavak.

Kiberneticka Inteligencija
Aktivnosti koje koriste sve izvore "inteligencije" u znak kiberneticke podrške, da se identifikuju opšte kiberneticke pretnje, da akumuliraju namere i kiberneticke vestine mogućih protivnika da se analizira i komunicira, kao i da identifikuju, lociraju i reagujući na izvorima kibernetickog napada.

Kiberneticki Terorizam To je svakodnevni I najatraktivniji izbor za teroriste, jer se može postići sa skromnim finansijskim sredstvima, anonimno i od velike udaljenosti. Kiberneticki terorizam predstavlja najveći potencijal za štetu kada se sjedinjava za fizičke napade. *Kiberneticki* epitet koja se ovde koristi posto terorista napada sa ili koristi tehnologiju.

Kriticne Infrastrukture (da se regulise)
Kritična infrastruktura je imovina i sistemi i institucije od velikog značaja za javno dobro, propust ili povrede od kojih će dovesti do održivih kontrakcija snabdevanja, značajnim narušavanjima javne bezbednosti ili drugih dramatičnih posledica.

U Zelenom dokumentu Evropskog Programa za zaštitu kritičke infrastrukture, Evropska Komisija daje indikativnu listu od 11 kritičnih sektora[5]:

[4]Evropska Komisija - http://ec.europa.eu/dgs/home-affairs/ëhat-ëe-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm
[5]Evropska Komisija – Zeleni Dokumenat za Evropski Program za Zastitu Kriticne Infrastrukture http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52005DC0576

- Energija
- Informaciona tehnologija i komunikacija (ITK)
- Voda
- Hrana
- Zdravlje
- Finansije
- Javni red i javna pravna bezbednost
- Civilna Uprava
- Prevoz
- Hemijska i nuklearna industrija
- Prostor i istraživanja

Kriticna Infrastruktura informacije (KII):
Sistemi KII koje su kritične infrastrukture za sebe ili da su od suštinske važnosti za funkcionisanje kritične infrastrukture (telekomunikacije, kompjuteri/softver, internet, sateliti, itd).

Zastita kriticne infrastrukture informacije (ZKII)
Programi i aktivnosti vlasnika, operatera, proizvođača, korisnika i regulatorne vlasti infrastrukture, koji su namenjeni za održavanje performanse kritične infrastrukture informacija u slučaju kvara, napada ili nesreća iznad jednog definisanog minimlanog nivoa usluga, čiji je cilj smanjenje vremena oporavka i smanjuje oštećenja.

CIIP -ra treba posmatrati kao međusektorski fenomen, nije pojava ograničena na određene sektore. CIIP -ra treba da budu usklađene sa zaštitu kritičke infrastrukture od opšte perspective.

Alarmisanje
Obaveštenje o mogućim situacijama i katastrofa koje mogu nastati, ili su se tamo dogodile. Uputstvo za primaoca da ostane spreman za bilo kakvu eskalaciju potencijalnih ili aktiviranja odgovarajućih relevantnih mera.

Ekipa Reagovanja prema Incidentima Kompjuterske Bezbednosti (ERIKB)
Ekpa reagovnja prema incidentima kompjuterske bezbednosti (ERIKB) je servis organizacija odgovorna za prijem, razmatranje i odgovor na incidente i druge aktivnosti protiv bezbednosti računara. Njegove usluge su obično za definisanje institucije koja može biti jedan maticni predmet, kao korporativne organizacije, vlade ili obrazovanja; regija ili država; istraživačka mreža; ili jedan plaćani klijenat.

ERIKB – moze biti jedna sluzbena ekipa ili *adhoc* ekipa. Formalna ekipa obavlja posao za reagovanje na incidente kao osnovnu karakteristiku. *Adhoc* ekipa prikupljena tokom incidentaa kompjuterske bezbednostiili da reaguje nakon prema potrebi.

Ekipe reagovanja prema kompjuterskim emergencijama (ERKE)
Ekipe za hitno reagovanje računara do (ERKE) su grupe stručnjaka koji se bave bezbednoscu računara. Drugi nazivi za takve grupe mogu biti Ekipe Pripravnosti za kompjuterske emergencije I ekipe za reagovanje prema incidentima kompjuterskih bezbednosti (ERIKB) .

Naslov"Ekipa Reagovnja prema Kompjuterskim Emergecijama" se uglavnom koristi od strane

[5] Komisioni Evropian – Dokumenti i Gjelbër për Programin Evropian për Mbrojtjen e Infrastrukturës Kritikehttp://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52005DC0576

Koordinacionog Centra ERKE (ERKE - CC) na Univerzitetu Karnegi Mellon (CMU). Skracenica ERKE istorijska oznaka, onda se koristila od sličnih ekipa iz celog sveta.

Evropska Agencija za Bezbednost Mreza i informacije (ENISA)

Evropska Agencija za Bezbednost Mreža i Informacija (ENISA) je agencija Evropske Unije (EU), stvorena da spreči i adresiranje problema o bezbednosti mreža i informacije.

2 Metodologija

Nacionalna Strategije za Kiberneticku Bezbednost je dizajnirana na osnovu procene i analize agencijama za sprovođenje zakona, vlade i lokalnih i međunarodnih organizacija, globalnim trendovima i praksama i politikama Evropske Unije. U tom kontekstu, strategija je u skladu sa instrukcijama ENISA i strategija država članica EU.

Radna grupa za izradu Strategije je formirana Odlukom Ministra Unutrašnjih Poslova br. 195/2015 od 05.06.2015 koja je obuhvatila sve državne institucije, profesionalna udruženja, civilnog društva i međunarodnih partnera.

Na prvom sastanku Radne grupe je dodeljena je jedna uza grupa za razvoj početnog nacrta Strategije. Ova pod grupa je održala nekoliko sastanaka i razvio prvobitni nacrt koji je prosleđen svim članovima. Strategija je izradjena osigurajuci potpunu transparentnost i uključivanje svih članova i predstavnika finansijskih institucija.

Strategija je izrađena aplicirajuci metodu upoređenja, pocetno analizirajuci izmene kiberneticke bezbednosti Kosova sa zemljama regiona na osnovu ove analize su identifikovane aktuelne mere koje treba preduzeti da bi se stvorio jedan mehanizam i drugim zemljama. Na osnovu ove analize su idenrifikovane aktuelne mere i onih koji treba da se preduzimaju da bi se stvorio jedan efektivni mehanizam u skladi sa globalnim trendovima da bi garantovao kiberneticku bezbednost u Republiku Kosovo.

Takođe ja analizirano teorijska lietartura iz oblasti kiberneticke bezbednosti i upotrebljeni su osnovni materijali kao osnova primarnih i sekundarnih izvora kao; analiza i procena rizika od strane drzavnih Institucija, objavnljivanja od strane lokalnih i međunarodnih organizacija, adaptirane strategije drzava clanica EU-je , uputstva ENISA, i ostala relevantna dokumentacija.

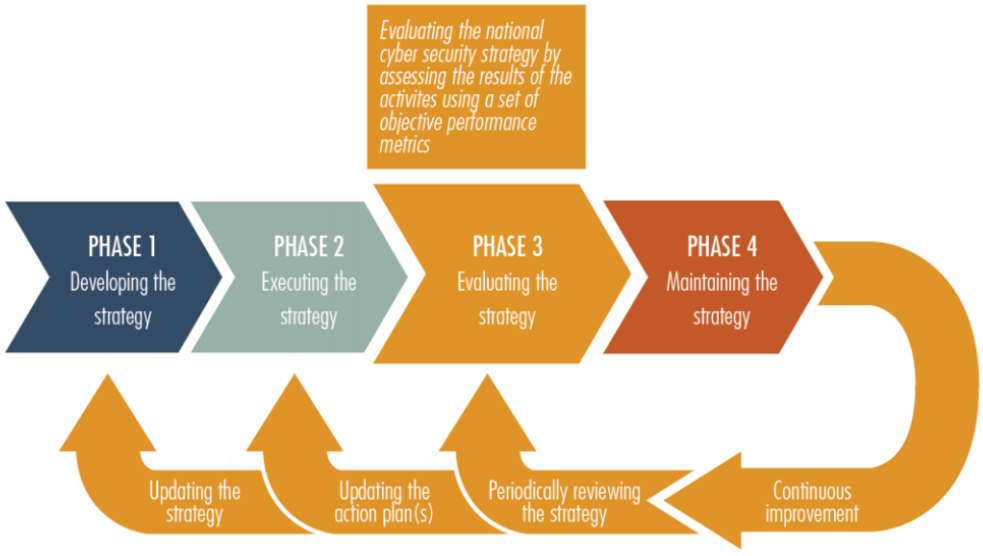
Od 21-23 oktobra radionica je održana u Bogi podržavana od ENCYSEC gde je pozvao sve institucije. Svi predstavnici su imali priliku da ponude svoje predloge i razgovaraju o aktivnostima Strategije i Akcionog Plana.

3 SistemMenadziranja Kiberneticke Bezbednosti

3.1 Zivotni Ciklus Strategije

Na osnovu ključnih preporuka međunarodnih tela (NATO, ENISA), Nacionalna Strategija za Kiberneticku Bezbednost treba da se razvija u okviru životnog ciklusa, koji obuhvata sledeće faze:
1. Razvoj;
2. Implementacija;
3. Evaluacija; i
4. Adaptacija Strategije.

Na taj način osigurava kontinuirani napredak strategije, procedure i proizvoda, a u skladu sa promenom okolnosti u neposrednom okruženju i šire.



Slika 1: Kiberneticku Bezbednost životnog ciklusa (Izvor: ENISA 2012)

3.2 Izazovi, rizici, pretnje prema bezednosti kibernetickog prostora na Kosovo

S obzirom da kiberneticki proctor je prostor za kriminalna zlouptrebljavanja, postoji niz rizika i pretnji koje ugrožavaju bezbednost ljudi u kibernetickom prostoru.

Mnogi od rizika i uticaja kibernetickih incidenata su zajedničke za vlade i privatnog sektora. Cilj strategije je da se ublaže rizici prema kibernetickoj bezbednosnih i da neće tolerisati one rizike koji imaju izuzetno visok uticaj.

Sa trenutnim saznanjima, osnovne rizici i preteći elementi koji se bave sa IKT sistemima u Republici Kosovo je napisane na sledeći način:

A. Pretnje

Kiberneticke pretnje dolaze od mogućnosti i namere neprijatelja da pokrene kiberneticki napad na sistemima komuniciranja i informacije.
Postoje četiri vrste kibernetickih napada:

- **Sabotaža**, kibernetcki napadi koji ometaju normalno funkcionisanje sistemima i informacijama.
- **Špijuniranje**: KIberneticki napadi koji se bave nesmetanim intervenisanjem treće strane u okviru komunikacionih sistema i informisanja, čitajuci, menjajuci, uklanjanjajuci ili dodavanje informacija. Takve intervencije mogu da se koriste za zloupotrebe napadnute sisteme komunikacije i informacija, kao i da napadne druge sisteme.
- **Terorizam:** Kiberneticki terorizam ima veze sa naporima da se ciljaju viši nivoi, napravljen sa terorističke svrhe koja je u toku pretnje i ima potencijal da izazove veliku štetu. Dok smo mi često povezivali sa terorizmom sa gubitkom života, ne možemo da previdimo važne posledice kao zastrašivanja ili impulse koji mogu biti izazvani od kibernetickog terorizma.
- Da se popunjava
  U budućnosti, čak i na operacijma, ali i za njene diplomate, Vlada može da se suoči sa neprijateljima koji imaju kapacitet ofanzive i kiberneticke inteligencije (reformulacija). Ovo bi donele realne rizike u tajnosti i integriteta podataka, kao i dostupnosti sistemima i informacijama.
  Radikalne i ekstremističke grupe sve više se koriste kiberneticki proctor za organizaciju i propagandu da promovišu svoje aktivnosti, regrutuju nove članove i organizuje terorističke akte, koji predstavljaju pretnju za nacionalnu bezbednost Republike Kosovo.
  Kritične infrastrukture informacije su u stalnosti meta kiberenetickih napada. Ovi napadi su posebno meta terorista i hakera koji traže osetljive informacije i

B. Rizici

Nepostojanje Nacionalnog Saveta Kiberneticke Bezbednosti sa svojim funkcijama;

- Neprestrojavanje državnog CERT-a i drugih u Trusted Introdicer[6] i FIRST[7];;
- Nedostatak znanja i razumevanja mogućnosti za digitalne napade koji predstavljaju realnu opasnost
- Nedostatak znanja i razumijevanja prilika za cyber napada koji čine stvarnu prijetnju.

C. Ugrozenost

Ne postoji odgovarajuća sigurnost i zaštitu u kiberntickom prostoru. Međutim, mogućnost kibernetickog napada je mnogo veći od fizičkog napada. Vlasti i obični građani na Kosovu su već bili žrtve skibernetickog napada, naravno takođe će se suočiti sa takvim napadima i u budućnosti. Jedan od najvećih izazova leži u povećanju svesti korisnika, jer većina njih koristi kiberneticki proctor prema svetskim statistikama, većina kibernetickih incidenata su izazvane zbog ljudske greške. Kao rezultat toga, unutrašnja pretnja je vrlo realna.

[6]Lista CERT-a/CSIRT-a u Trusted Introducer - https://www.trusted-introducer.org/directory/country_LICSA.html
[7]Lista clanova FIRST-a - https://www.first.org/members/teams

Uprkos ograničenog direktnog uticaja, rizici koji se odnose na kiberneticke napade ne mogu se potceniti.

3.3 Adresiranje kibernetickog kriminala

Potreba za blisku saradnju između organa za sprovođenje zakona širom sveta je hitno da se bori protiv brzog rasta kibernetickog kriminala.

Kiberneticki kriminal će biti jedan od najvažnijih izazova za Institucije Republike Kosova u celini, a posebno Kosovska Policija. Republika Kosovo je preduzela konkretne korake u uspostavljanju pravne infrastrukture za sprečavanje i borbu protiv svih oblika kiberntickog-kriminala, ali i dalje postoje mnogi izazovi, posebno u tehničkom smislu uspešna suočavanja sa ovim oblikom kriminala na Kosovu je relativno novi fenomen.

Značajno povećanje broja korisnika Interneta u poslednjih nekoliko godina na Kosovu je doveo sa povećanja rizika od kriminala i kibernetickog napada. Neke kriminalne aktivnosti koje imaju su se desile su dovoljne da se istakne ranjivost računarskih mreža u zemlji i za koje se smatra das u i dalje u fazi razvoja.

Prema raspoloživim podacima, glavne mete kibernetickih napada na Kosovu do danas su računi korisnika, bankarski sistemi, i veb stranice na internetu.
Potrebno je dodatno ojačati kapacitete agencija za sprovođenje zakona u borbi protiv visokotehnološkog kriminala, kao iu pogledu zaštite špijuniranja i sabotaže. Takođe, moramo da se unapredimo mehanizam Kosovske Policijska Služba za borbu protiv visokotehnološkog kriminala, podržavajući njihovo saradnju sa međunarodnu razmenu informacija i obuke. Pored toga, postoji potreba da se obezbedi stručno usavršavanje i obuka policijskih stručnjaka, stvarajući multidisciplinarno akademsko okruženje, kako bi se unapredili kapaciteti Kosovske Policije u potrazi za kiberntickim-kriminalom.

Kibernticki criminal zahteva od institucije za reakcije specijalizovanih pravosudnih organa i Agencija za sprovođenje zakona i tužioca da moraju biti u stanju da preduzmu istragu i gonjenje krivičnih dela protiv podataka i računarskih sistema, dela počinjenih od strane računara i elektronskih dokaza koji se odnose na krivična dela.

3.4 Balansiranje bezbednosti i privatnosti

Javne vlasti i privatne, u skladu sa Ustavom Republike Kosovo, osiguraju poštovanje ljudskih prava i osnovnih sloboda. Osnovna prava moraju biti garantovana I unutar kibernetickog prostora. Povecanje kiberneticke bezbednosti ne mogu poboljšati zastitu privatnost i imovine korisnika u kibernetickom.

Vlada Republike Kosovo će nastaviti da preduzme neophodne mere da garantuju zaštitu i kiberneticku bezbednosti države. Ove mere će poštovati prava na privatnost i osnovne slobode, pristup informacijama i drugim demokratskim principima.

4 Opšti principi

Struktura i sadržaj ovog dokumenta zasniva se na ovim principima:

Princip ustavnosti i zakonodavstva- preduzete radnje za poboljšanje kiberneticke bezbednosti moraju biti zasnovana na odredbama utvrđenim Ustavom Republike Kosov, zakonodavstvu i međunarodnim sporazumima.

Princip Državne bezbednosti – kibernetika bezbednost je sastavni deo države, podržava funkcionisanje države i društva, ekonomske konkurentnosti i inovativnosti. Ovaj princip podrazumeva zaštitu prava na bezbednost i zaštitu za sve građane sprečavanjem visokotehnološkog kriminala.

Princip odgovornosti - zbog vlasništva i funkcionisanja različitih sistema informacione i komunikacione tehnologije, država ne može snositi odgovornost samo za zaštitu kibernetickog prostora i prava građana na Internetu. Vlasnici i operateri informacione i komunikacione tehnologije imaju primarnu odgovornost za zaštitu svojih sistema i podatke svojih korisnika.

Princip sveobuhvatnog pristupa –je od suštinskog značaja da razvije sveobuhvatan pristup u suocavanju sa pretnjama u kibernetickom prostoru.

Princip javno-privatnog partnerstva- kiberneticka bezbednost se omogućava na koordiniran način, kroz saradnju između javnog i privatnog sektora, s obzirom na povezanost i međuzavisnost postojeće infrastrukture i usluga u kibernetickom prostoru.

Princip kontinuiteta- aktivnosti treba da se podele kao deo strategije u kontinuitetu. Ovo je posebno važno jer će biti administrativnih rokovia proceduralni put, i zbog delovanja različitih inicijativa moraju biti povezane sa akcijama koje će nastaviti godinama.

Princip povjerljivosti - institucija sa odgovornostima u prevenciji i borbi protiv visokotehnološkog kriminala trebaju da stvoei poverenje u zaštiti istraga, podataka i integritet informacija od zloupotrebe od strane onih koji imaju pristup do njih.

Princip ljudskih prava i sloboda – kiberneticka bezbednost se garantuje uz poštovanje ljudskih prava i osnovnih sloboda, kao i zaštitu individualnih sloboda, ličnih podataka i identiteta, bez obzira na etničku pripadnost, pol, starost, religiju i seksualne orijentacije.

Princip međunarodne saradnje – kiberneticka bezbednost se unapredjuje kroz međunarodnu saradnju sa partnerima i saveznicima. Kroz saradnju, Republika Kosovo će igrati ključnu ulogu u promovisanju globalne kiberneticke bezbednosti.

5 Pravni Okvir i Institucionalni Mehanizmi

5.1 Pravni Okvir

U oblasti kiberneticke bezbednsoti, Republika Kosovo sptovodi jednu široku zakonsku osnovu, koja uključuje, ali nije ograničeno na:

Ustav Republike Kosova[8];
Zakon br. 03 / L-050 o osnivanju Saveta Bezbednosti Kosova[9];
Zakon br.03 / L -166 Sprečavanje i Borba Protiv KIbernetickog Kriminala[10];
Zakon br. 04 / L-145 o Vladinim Organima i Informacionog Društva[11];
Zakon br. 04 / L-094 o Uslugama Informacionog Društva[12];
Zakon br. 04 / L-109 o Elektronskim Komunikacijama[13];
Zakon br. 05/l-030 o presretanju elektronksih komunikacija[14]
Zakon br.03 / L - 172 o Zaštiti Ličnih Podataka[15];
Zakon br. 04 / L-076 o Policiji[16];
Zakon br. 03 / L-142 o Javnom Redu i Miru[17];
Zakon br. 03 / L063 o Obaveštajnoj Službi Kosova[18];
Zakon br. 04 / L-149 o Izvršenju Krivičnih Sankcija[19];
Zakon br. 04 / L-065 o Autorskim i Srodnim Pravima[20];
Zakon br. 03 / L-183 o Sprovođenju Međunarodnih Sankcija[21];
Zakon br. 04 / L-213 o Međunarodnoj Pravnoj Pomoć u Krivičnim Delima[22];
Zakon br. 04 / L-052 o Međunarodnim Sporazumima[23];
Zakon br. 04 / L-072 o za Kontrolu I nadzaor Granice[24];
Zakon br. 04 / L-093 o Bankama, Mikrofinansijskim Institucijama i Nebankarske Finansijske Institucije[25];
Zakon br. 04 / L-064 o Kosovskoj Agenciji za Sudsku Medicinu[26];
Zakon br. 04 / L-198 o Prometu Strateških Roba[27];
Zakon br.04 / L -004 o Privatnim Službama Bezbednosti[28];
Zakon br. 03 / L-046 o Sigurnosnim Snagama Kosova[29];

[8] http://gzk.rks-gov.net/ActDetail.aspx?ActID=3702
[9] https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=2521
[10] https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=2521
[11] https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=2851
[12] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2811
[13] https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=2851
[14] https://gzk.rks-gov.net/ActDetail.aspx?ActID=10968
[15] http://gzk.rks-gov.net/ActDetail.aspx?ActID=2676
[16] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2806
[17] http://gzk.rks-gov.net/ActDetail.aspx?ActID=2651
[18] https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=2538
[19] https://gzk.rks-gov.net/ActDetail.aspx?ActID=8867
[20] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2787
[21] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2674
[22] https://gzk.rks-gov.net/ActDetail.aspx?ActID=8871
[23] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2789
[24] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2801
[25] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2816
[26] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2781
[27] https://gzk.rks-gov.net/ActDetail.aspx?ActID=8860
[28] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2741
[29] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2523

Kod br. 03 / L-109 o Carini i Akcizama na Kosovu[30];
Zakon br. 04 / L-099 o Izmenu Zakona o Carinama i Akcizama na Kosovu, br. 03 / L-109[31];
Zakon br.03 / L-178 o Klasifikaciji Informacija i Verifikaciji Bezbednosti[32];
Kod br. 04 / L-082 Krivičnog Zakonika Republike Kosovo[33];
Kod br. 04 / L-123 o Krivičnom Postupku[34];
Zakon br.03 / L-122 za Spoljnu Službu Republike Kosova[35];
Kod 03 / L-193 o Maloletničkom Pravosuđu[36];
Uredba br.18 / 2011 za Distribuciju i Prenos Poverljivih Informacija[37].

Ova strategija je u skladu sa međunarodnim zakonima koji regulišu kiberneticku bezbednost, Strategija Evropske Unije: Otvoreni prostor, siguran kiberneticki zašticen (2013)[38]; Smernice za ENISA za Dzavnu Strategiju KIberneticke bezbednostii (2012)[39]; KIberneticka bezbednost drugih zemalja EU .

5.2 Institucionalni Mehanizam

Institucionalni mehanizam podrazumeva sve mehanizme koji imaju ulogu i značaj u kibernetickoj bezbednosti na Kosovu.

Institucionalni mehanizmi za razvoj i implementaciju državne politike u oblasti kiberneticke bezbednosti su, ali ne ograničavajući se na:

Nacionalni Koordinator za Kiberneticku Bezbednost
Nacionalni Koordinator za KIberneticku Bezbednost je Ministar Unutrašnjih Poslova, ili lice koje on ovlasti, koja je odgovorna za koordinaciju, vodi, prate i izveštavaju o sprovođenju politike, aktivnosti i akcije koje se odnose na Strategiju Kiberneticke Bezbednosti.

Sekretarijat
Sekretarijat ima za funkciju prikupljanje informacija i podataka od drugih institucija, analizu i procenu prikupljenih informacija, kao i razvoj analitičkih izveštaja za Nacionalnog Koordinatora i Nacionalnog Saveta Kiberneticke Bezbednosti. Pored toga, Sekretarijat će distribuirati pravovremene informacije svim relevantnim stranama, čime podržava Akcioni Plan za kiberneticku bezbednost.

Ministarstvo Unutrasnjih Poslova
MUP ima vodeću ulogu u koordinaciji strategije, praćenje provedbe Akcijskog plana i nacrt periodična izvješća. MUP je također odgovoran za formuliranje i praćenje politike i zakonodavstva u području opće sigurnosti i cyber sigurnosti. Kosovska policija provođenje zakona agencija unutar

[30] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2600
[31] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2600
[32] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2690
[33] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2834
[34] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2861
[35] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2615
[36] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2698
[37] http://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=10554
[38] Strategija Kiberneticke Bezbednosti Evropske Unije http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
[39] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

Ministarstva unutarnjih poslova, ima glavnu odgovornost u borbi protiv svih oblika cyber kriminala, preko Odjela za cyber kriminal i ostalih pratećih objekata u sklopu Kosovske policije. BP će također poslužiti kao točka kontakta Resident 24/7 na međunarodnoj suradnji u području cyber kriminala.

Sudski Savet Kosova
Osigura da Sudovi na Kosovu budu nezavisni, profesionalni i nepristrani, sa ciljem da sudski sistem bude sto efikasniji u borbi protiv kibernetickog kriminala.

Tuzilacki Savet Kosova
Osigura da tuzilacki sistem na Kosovo bude nezavisan, nepristran i profesionalan i sprovođenju gonjenja, istrage i otkrivanja krivicnih dela kibernetickog kriminala i da predstavlja u sudovima optuzenicke akte u ime drzave.

Tuzilastva i Sudovi
Su odgovorne institucije za gonjenje krivicnih dela, njihovo adekvatno kanjavanje, za konfiskaciju imovine i drugih aseta dobijenih putem kriminalnih aktivnosti.

Sekretarijat Saveta Bezbednosti Kosova
Sekretarijat, kao deo Saveta Bezbednosti Kosova vrsi pripremanje preiodicnih izvestaja I analiza Valde Republike Kosovo I Saveta Bezbednosti Kosova koji se bace pitanjima politike bezbednosti kao I pruza pomoc u izradu politika bezbednosti Republike Kosovo, ukljucuvisi I izgradnju kapaciteta, instrumente politika iztrazivanja, pruzanje administrativne podrske I funkcionalne Saveta Bezbednosti Kosova.

Obavestajna Sluzba Kosova
OSK vrsi identifikaciju pretnji koje rizikuju bezbednost Kosova. Pretnju prema bezbednosti Kosova se smatra pretnja prema teritorijalnom integritetu, integritetu institucija, ustavnog poretka, stabilnosti i privrednog razvoja, kao i pretnje prema globalnoj bezbednosti na stetu Kosova.

Ministarstvo Pravde
MP priprema I razvija zakonodastvo u obalsti pravde I koordinira I razvija pravnu međunarodnu saradnju u krivicnim pitanjima.

Ministarstvo za Sigurnosne Snage Kosova
MKSF razvija i jača cyber sigurnost informacijskih sustava, komunikacije i članstvo MKSF/KSF strane, Chat ono sustavi se koriste za obavljanje poslova na ustavnom skladu misija članstva. KSF mogu sudjelovati u potpori civilnim vlastima u zaštiti podataka i kritične infrastrukture u slučaju krize u zemlji.

Ministarstvo za Ekonmski Razvoj
Osigurava kvalitete usluga i tehničkih standarda u području telekomunikacija, razviti politike za promicanje konkurencije u telekomunikacijskom području, istražuje potrebe i zahtjeve kupaca u telekomunikacijama, podržava informacijske tehnologije i inovacije, podržava pristup tehnologiji na svi građani Kosova i poticati razvoj obuke informacijskih sustava tehnologije.

Ministarstvo Finansija
MF preko carina, Obavestajne i finansijske jedinice, I Poreske Administracije ce pomoci u jacanju kiberneticke bezbednosti I sprecavanju o susbijanje kibernetickog keiminala

Ministarstvo Obrazovanja, Nauke i Tehnologije
MONT igra vaznu ulogu u sprecavanju I budjenja svseti preko izrade kurikula, organizovanja aktivnosti bidjenja svesti za koriscenje ineterneta I drugih van-programskih aktivnosti

Ministarstvo Spoljnih Poslova
MSP ima ulogu u pravsu davanja pomoci za medjunarodnu saradnju u borbi protiv organizovanog kriminala.

Ministarstvo za Evropske Integracije
MEI osigura pravne okvire I politike Vlade Republike Kosovo su u skladu sa zakonodavstvom I politikama EU-je.

Regulatroni Autoritet Elktronskih i Postanskih Komunikacija
RAEPK je regulatroni organ, koji sprovodi i nadzire regulatorni okvir da utvrdjena zakonomë za Elektronske Komunikacije, iz zakona za postanske usluge, kao i iz politika razvoja u obalsti elektonskog komuniciranja i postanskih usluga.

Agjencia za Drstvo informacije
ADI vrsi kordinaciju I nadzor procesa I mehanizama elektronskoe vladavine u vezi sa infrastrukturom TIK, prosirivanjem usluga internet I sadrzaja internet u institucijama republike Kosovo, akumulisanje, administriranje, prosirivanje I cuvanje podataka stvarajuci Drzavni centar elektronskih podataka kao I Bezbednost I zastitu Elektronske komunikativne Infrstaukture I podataka. ADI prema potrebi pomaze relevantne institucije u borbi kibernetickog kriminala I osigura zastitu licnih podataka u elektronskoj formi, u skladu sa zakonodavstvom na snazi.

Drzavna Agencija za Zastitu Licnih Podataka
DAZLP osigura kontrolere da postuju njihove obaveze oko zastite licnih podataka kao I subjekti podatak budu informisani oko njihovih prava I obaveza u skladu sa Zakonom za zastitu Licnih Podataka. Takodje pruza savete za Skupstinu republike Kosovo, Vladu, drzavnim organima lokalne vlasti I svim sprovodnicima javne vasti na Kosovo u vezi sa pitanjima za Zastitu Licnih Podataka, kao I savetuje sve privatne institucije u vezi sa Zastitom Licnih Podataka.

6 Ciljevi Strategije Kiberneticke Bezbednosti

Nacionalna Strategija za KIberneticku Bezbednost ima sledeće strateške ciljeve:

1. Zaštita kritične informacione infrastrukture;
2. Institucionalni razvoj i jačanje kapaciteta;
3. Izgradnjajavno-privatno partnerstva;
4. Reagovanje na incidentima;
5. Međunarodna saradnja .

6.1 Zastita kriticne informacione Infrastrukture

Ova strategija ima za cilj da stvori bezbednost kibernetickog prostora u Republici Kosovo, sa konkretnim akcijama i merama za zaštitu kritične informacione infrastrukture, prekida ili uništenja od kojih bi imalo ozbiljne posledice prema društvenim vitalnim funkcijama.

Zaštita kritične informacijske infrastrukture bit će dio Zakona o identifikaciji i zaštitu kritične infrastrukture koji će biti sastavljen u 2016. Javni i privatni sektor treba da stvori jednu unapredjenu stratešku bazu i organizacionu na osnovu intenziviranja razmene informacija. Ukoliko je potrebno, i u slučaju specifičnih pretnji, biće potrebne zaštitne mere. Pored toga, ona će takođe proceniti potrebu usklađivanja pravila za održavanje kritične infrastrukture tokom tehnoloških kriza.

6.1.1 Identifikacija kriticne informacione Infrastrukture

Neophodno je da se identifikuje i proceni kritična infrastruktura u Republici Kosovo za najbolju moguću zaštitu. Kritična infrastruktura će biti identifikovana i vrednovana na osnovu niza utvrđenih kriterijuma, uzimajuci u obzir dokumenat *metoddologija* ENISA *za utvrđivanje dobara i usluga ključne informacione*[40] *infrastrukture.*

Koraci koje treba slediti za identifikaciju kritične informacione infrastrukture obuhvataju sledeće:
• **Određivanje sredstava** koje ce biti tretirane (na primer, vokalne komunikacije, prenos podataka, skladištenje i obrada podataka) koje se mogu klasifikovati kao kritičane;
• **Identifikacija infrastrukture** koja je neophodna za tehničko funkcionisanje ovih službi;
• **Uspostavljanje objektivnih kriterijuma** za nivo zaštite koja je potrebna za svaki element infrastrukture, kategorizaciji infrastrukture i korišćenja kriterijuma kao što su broj dotaknuih korisnika, nivo osetljivosti informacija koje se koncentrisu, cuvaju, prenose ili prerađene u tim infrastrukturama itd;
• **Ispitivanje kriterijuma** za razvoj scenarija koji uzimaju u obzir poremećaj funkcionisanja odabrane infrastrukture, u okviru redovnih aktivnosti.

[40]ENISA https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/Methodologies-for-identification-of-ciis

6.2 Institucionalni razvoj i jačanje kapaciteta

6.2.1 Odredjivanje Nacionalnog Koordinatora i zadaci Drzavnog Saveta za Kiberneticku Bezbednost

Posto pristup mehanizmima zaštite je višestruka, važno je razumeti i prepoznati da je održavanje prihvatljivog nivoa bezbednosti u KIbernetickom prostoru se može postići samo kroz saradnju između različitih strana uključenih u okviru koordinisanog odgovora i različitih pretnji koje su već pomenute u poglavlju 3.

Koordinacija relevantnog nadležnog organa ili vlasti je apsolutno neophodna. Ova koordinacija je produktivna kada ga vrši entitet koji je u stanju da organizuje i koordinira različite aktere i akcije u Republiku Kosova, za ispravan odgovor na pretnje koje se danas pojavljuju, kao i prema novim pretnjama u kibernetickom prostoru.

Državni Savet KIberneticke Bezbednosti treba da uspostavi i da ojača saradnju u okviru javnih vlasti i saradnje između javnih vlasti sa privatnim sektorom, kao i da daju preporuke o strateškim pitanjima na najvišim političkim nivoima.

Savet čine predstavnici sledećih institucija: Ministarstvo Unutrašnjih Poslova, Policije Kosova, Kosovska Agencija za Forenziku, Ministarstva Bezbednosnih Snaga Kosova, Kosovske Obaveštajne Agencije, Agencije za Informaciono Društvo, Savet Bezbednosti Kosova, Ministarstva Pravda, Tužilački Savet Kosova, Sudski Savet Kosova, Ministarstvo Finansija, Carinska Služba, Ministarstvo Obrazovanja, Nauke i Tehnologije, Ministarstva Spoljnih Poslova, Regulatorni Organ za Elektronsku i Poštansku Komunikaciju, Centralna Banka Kosova. U posebnim slučajevima, biće uključivane i ministarstva, agencije i druge institucije.

Predstavnici privrede će biti pozvani kao članovi po potrebi. Akademski predstavnici će takođe biti angažovati u tehničkom nivou. Nacionalni Savet Kiberenticke Bezbednosti ima za cilj da koordinira sa preventivnim sredstvima i interdisciplinarnim pristupima KIbernetickom prostoru u javnom i privatnom sektoru.

6.2.2 Izgradnja kapaciteta u sekretarijatu za Strategije

Da se osigura monitorisanje i koordiniranje aktivnosti Strategije je neophodno da se regrytuje jedan sluzbenik u Sekretarijatu Strategija. Ministarstvo Unutrasnjih Poslova do treceg kvartala 2016 godine ce zvrsiti sve proceduren objavljivanja regrutacije relevantnog sluzbenika

Takodje uz podrsku medjunarodnih partnera ce biti organizovane obuke i studijske posete sa ciljem podizanja kapaciteta relevantnih sluzbenika.

6.2.3 Budjenje Svesti

Radit će se za promovisanje jedne kulture kiberneticke bezbednosti u celom društvu, uključujući i saradnju sa obrazovnim sistemom, industrijom, kao i promovisanje organizacije kao mesec

Evropske KIberneticke Bezbednosti. Posebnu pažnju treba obratiti na državne službenike, nove generacije, kao i korisnike interneta i kontinuirane isporuke novih programa za informacionu bezbednost u svim nivoima obrazovanja, sa ciljem korišćenjem naprednih informacionih sistema.

Ove potrebne mere koje treba preduzeti da bi se olakšalo: i:
• Upravljanje stručnost i znanje u oblasti Interneta. Fleksibilna adaptacija obuke neophodna u odnosu sa brzim pretnjama i stalno razlicite;
• Učešće u nacionalnom i međunarodnom simulacijama, obuke (radionice, kursevi i dr). Pružanje programa za kiberneticku bezbednosti jedna program vežbi za kiberneticku bezbednost za testiranje i specifikaciju mogucnosti reakcije na događaje. Domaće i međunarodne vežbe igraju važnu ulogu u razvoju i evaluaciju Kiberneticke bezbednosti;
• Načini budjenja svesti (npr. učenje) i informativne kampanje će biti ponuđene svim građanima Kosova;
Pružanje odgovarajucih kurseva za sve uključene strane: unutar organizacija koje su nagazovane spolja, u domaćem i međunarodnom partnertitetu (npr. učešća u raznim aktivnostima obuke). Važno je da rukovodioci u organizacijama imaju dovoljno znanja u oblasti kiberneticke bezbednosti. Zato kiberneticke aspekte treba uključiti u postojeće obrazovne programe Kosova.

6.2.4 Pravna Infrastruktura
Glavni je cilj usklađivanje pravnog okvira s Europskom unijom. U tom kontekstu, 2016 izradit će se po prvi Zakon o identifikaciji i zaštitu kritične infrastrukture. Važan dio ovog zakona će biti od kritičnih informacija zaštite infrastrukture.

Nadalje, to je identificiran kao nužno preispitati Zakon o sprečavanju i borbi protiv kibernetičkog kriminala, te izrađuje zakone koji pokrivaju područje cyber sigurnosti.

Zakonski okvir će se izmijeniti i uskladiti Nacionalnim planom za provedbu Sporazuma o stabilizaciji i pridruživanju.

6.2.5 Ljudski Kapaciteti
Sa ciljem uskladjivanja aktivnosti i obuke svih institucija ukljucene u ovoj Strategiji, bice izradjene kirukule obuke, glavni cilj je organizovanje obuka sa ciljem poboljsavanja koordinacije ukljucenih institucija, ali ce biti organizovane i specificne obuke za jednu ili vise grupa institucije.

Vazabn deo je izrada skenarija i odrzavanje zajednickih obuka, preko kojih ukljucene institucije ce testirati njihove kapacitete u reagovanju prema raznim izazovima. Odrzvanje ovih vezbi ce bitno poboljsati reagovanje prema raznim pretnjama, bilo da su na institucionalnom ili lokalnom nivou.

6.2.6 Tehnicka Infrastruktura
Tehnicka infrastruktura igra vaznu ulogu u jacabju kiberenticke bezbednosti u Republiku Kosovo i sve institucije ukljucenih i posvecene da ce unapredjivati sisteme informacione tehnologije.

Izmddju ostalog, RAEPK ce osnivati platformu za prijem i registrovanje kibernetickih incidenata dok Kosovska Policija ce unaprediti opremu za iztragu kiberenetickog kriminala.

6.2.7 Istraživanje i razvoj

Republika Kosovo će nastaviti da intenzivira istraživanja o bezbednosti IT i zaštite kritične infrastrukture. Istraživanje i razvoj kapaciteta da se podigne unutar Kosova, i da će se koristiti za učešće u domaćim i međunarodnim projektima, u skladu sa raspoloživim sredstvima.

Istraživanje i razvoj su ključni za poboljšanje odgovora Kosova prema pretnjama Kiberneticke bezbednosti.

6.3 Izgradnja javno-privatnog partneriteta (JPP)

6.3.1 Podizanje saradnje u privatnom sektoru

Pošto je najveći deo kritične informacione infrastrukture pripada privatnom sektoru, neophodno je jasno definisati saradnju sektora u oblasti kiberneticke bezbednosti.

Konkretno, trebalo bi uspostaviti procedure za razmenu informacija sa:

- Provajderima Interneta;
- Bankarskim sektorom;
- Energetskim sektorom;
- Sektorom za snabdevanje vodom;
- Trasnportom (vazdusnimi kopnenim);
- Akademsku oblast. .

Bice organizovane zajedničke aktivnosti za obrazovanje o kibernetickoj bezbednosti, koja će se fokusirati na pružanje saveta o kibernetickoj bezbednosti nastavnog plana i programa, koja se odnosi na sertifikaciju stručnjaka informacionih bezbednosti i dalji razvoj nastavnih modula.

6.4 Reagovanje prema incidentima

6.4.1 Funksionalizacijaa drzvanog CERT/CSIRT i osnivanje drugih CRT/CSIRT-a na Kosovo

S obzirom na bezbednosnu spremnost se najbolje postiže sa upozorenjem I ranom prevencijom, Ekipe za Emeregentna Kompjuterska Reagovanja će dostaviti svoje izveštaje Sekretarijatu Oorgana na redovnoj osnovi, kao i za odvojene incidente. Ako kiberneticka bezbednosna situacija dostigne na nivou moguće krize ili se desilo, Sekretarijat će obavestiti direktno Državni Organ za kiberneticku bezbednost, na čelu sa Nacionalnim Koordinatorom.

Obezbeđivanje potpune funkcionalnosti ekipa za Emeregentna Kompjuterska Reagovanja (CERT / CSIRT) na Kosovu je sastavni i vitalni deo ove strategije, ali i ispunjavanje posvecenosti Vlade. Glavne funkcije CERT / CSIRT su sprečavanja ozbiljnih incidenata u vezi sa bezbednosti mreža i informacija, kao i neposredan odgovor i praktično tih incidenata kada do njih dođe.

Treba napomenuti da je za pravilno funkcionisanje CERT / CSIRT-potrebno je:

- neophodna infrastruktura, i
- osoblje sa naprednim relevantnim usavršavanjem.

Politika treba da sadrži praktične korake koje organizacija treba da preduzme kada se desava jedan incident u kibernetickoj bezbednosti. Zadaci u tretiranju incidenata zabeleženih su prvenstveno usmerene na pružanje sredstava informacija, - uz minimiziranje štetu u najkraćem mogućem roku. Pored pružanja trenutne zaštite da se suoči sa zadacima u incidentu koje će pojačati učenje organizacije, i može da pomogne u krivičnom gonjenju i istrage kriminalaca u oblasti kiberneticke bezbednosti. Dobra je praksa da vrsi vežbe za suočavanje sa incidentima, kao i stalno ažuriraju procedure, tako da kada je to neophodno u realnim situacijama, da su standardizovane, proverene i pouzdane.

6.4.2 Listovanje i akreditacija CERT-a u Trusted Indroduced i First

Detaljna objašnjenja kako napraviti popis na Trusted Introducer[41] i FIRST[42] uvoditelj i dostupan je na svojim web stranicama. Oglas je obvezna zahtjev i to je prvi korak da postane akreditirani i tako ima pristup uslugama samo članovima

6.5 Medjunarodna saradnja

6.5.2 Organizovanje i ucesce u medjunardnim organizovanjima

6.5.2 Unapredjivanje medjunarodne saradnje

Globalna kiberneticka bezbednost se može postići samo putem koordinisanja na nacionalnom i međunarodnom nivou. Kosovo će igrati aktivnu ulogu u međunarodnoj saradnji na evropskom i globalnom nivou, posebno u razmeni informacija, formulisanje međunarodnih strategija, razvoj dobrovoljnih šema i pravnih normi, gonjenje krivičnih dela, održavajući medjunarodne vezbe, i učešće u obuci i projektima saradnje.

Na nivou EU, mi ćemo podržati odgovarajuće mere u okviru Akcionog Plana za zaštitu kritične infrastrukture informacija, širenje i umereno povećanje mandata Evropske Agencije za bezbednost mreža i informacija (ENISA) u pogledu promenjlivog stanja pretnji u IKT I I sjednijvanje kompetentnosti u IT u institucijama EU. Strategija EU za nacionalnu bezbednost i Digitalnu Agendu daju smernice za druge aktivnosti.

Kiberneticka spoljna politika će se uklopiti na način i u interesu i državnih ciljeva za kiberneticku bezbednost da se koordiniraju i razvijaju u skladu sa politikom međunarodnih organizacija, kao što su ENISA, OEBS, Savet Evrope, OECD-a i NATO-a. Kosovo će ponuditi doprinos anti-botnet aktivnosti širom sveta.

[41] https://www.trusted-introducer.org/processes/registration.html
[42] https://www.first.org/membership/process

7 Implementacija, monitoring i procena Strategije

7.1 Uloga sistema monitoringa

Proces implementacije Strategije će nastojati na ispunjavanje strateških ciljeva i aktivnosti koje su specifične za njih. Monitoring i procena efikasnosti sprovođenja ciljeva i aktivnosti će biti sastavni deo procesa strategije, kao i ključne elemente u ispunjavanju svojih dužnosti. Monitoring i evaluacija su sredstva za merenje napretka u odnosu na određenim ciljevima, za procenu potreba za uspostavljanjem pravila upravljanja, naročito aktivnosti. Proces praćenja će voditi institucije, uz široko učešće drugih zainteresovanih strana.

Glavne dimenzije monitoringa i evaluaciju strategije su:
- institucionalni kapacitet;
- Indikatori monitoringa uzduž i na kraju perioda od tri godine;
- izvori informacija i merni instrumenti.

7.2 Institucionalni Kapaciteti za monitoring i procenu

Sistem monitoringa i evaluacije će biti proširen da obuhvati sve institucije koje su odgovorne za realizaciju ciljeva koji su definisani Strategijom i Akcionim Planom.

- Nacionalni Koordinator za kiberneticku bezbednost, kao vodeća institucija za ispunjenje ciljeva, indikatori će pratiti bezbednosnu strategiju kiberneticke bezbednosti. Na kraju svake godine, on će pripremiti izveštaj o napretku ciljeva.
- Ministarstva i druge institucije navedene u Akcionom Planu će biti odgovorne za monitoring i evaluaciju aktivnosti koje se izdvajaju za ta ministarstava ili njihovih podređenih institucija. Ove institucije će dostaviti svoje periodične izveštaje Nacionalnom Koordinatoru za kiberneticku bezbednost, tako da izveštaji budu standardizovani.
- Nevladine organizacije će učestvovati u monitoring i evaluaciju strategije, u okviru okruglih stolova održanih od strane Nacionalnog Koordinatora za kiberenticku bezbednost. U ovim okruglim stolovima, nevladine organizacije i civilno društvo će predstaviti svoju procenu i preporuke u vezi sa situacijom u oblasti kiberneticke bezbednosti.

7.3 Indikatori za monitoring i procenu

- Broj relevantnih zakona i propisa, koji je stupio na snagu nakon usvajanja Strategije;
- Uspostavljene Strukture (Koordinator, Organ, Sekretarijat);
- Broj zaposlenih obučenih u relevantnim institucijama za kiberneticku bezbednost;
- Oblasti nastavnog plan i udžbenici koji se bave pitanjem kibereneticke bezbednosti;
- Broj projekata i programa za kiberneticku bezbednost;
- Broj izveštaja monitoringa i evaluacije od strane državne strategije o kiberenetickoj bezbednosti;
- Broj međunarodnih aktivnosti za kiberneticku bezbednost.

7.4 Instrumenti za monitoring i evaluaciju

• Administrativni podaci / statistika iz različitih interesnih grupa kiberneticke bezbednosti;
• i izveštaj sprovodjenja Strategije;
• Istraživanja o nivou znanja građana Kosova kao rezultat različitih kampanja za podizanje svesti o kibernetickoh bezbednosti.

8 Akcioni Plan 2016-2019

Akcioni Plan je izrađen u okviru opšteg strateškog okvira utvrđenog sa Nacionalnom Strategijom za kiberneticku bezbednost.

Akcioni Plan će biti razmotren na kraju svake godine kako bi se osigurala održivost Strategije i usklađenosti sa nacionalnim i međunarodnim trendovima.

Akcioni Plan za sprovođenje ove strategije uključuje:

- Strateške ciljeve;
- Specifične ciljeve;
- Konkretne aktivnosti za implementaciju;
- Definisanje i podršku institucije odgovorne za ispunjavanje svakog cilja;
- Specifikacija roka za ispunjenje svake aktivnosti;
- Utvrđivanje potrebnih finansijskih sredstava za razvojne aktivnosti;
- Definisanje indikatora za realizaciju svakog cilja i aktivnosti.

Akcioni Plan odražava njenu usklađenost sa opštim okvirom Nacionalne Strategije za kiberenticku bezbednost Republike Kosovo.

Državna Strategija za kibernetičku bezbednost 2016 – 2019						
Strateški cilj 1 **Zaštita kritične infrastrukture informacije**						
Strateški cilj 2 **Razvoj institucionalnog i pravnog okvira i izgradnja ljudskih i tehničkih kapaciteta**						
2.1	**Specifični cilj: Određivanje nacionalnog koordinatora i dužnosti državnog saveta za kibernetičku bezbednost**					
Br.	**Aktivnosti**	**Rok**	**Budžet**	**Odgovorne institucije**	**Institucije koje podržavaju**	**Pokazatelji performanse**
2.1.1	Donošenje odluke od strane Nacionalnog koordinatora za osnivanje	K1 2016	Administrativni troškovi	MUP	Relevantne institucije	Potpisana odluka
2.1.2	Organizovati redovne sastanke svaki treći mesec	2016-2019	Planirani troškovi	Nacionalni koordinator	Relevantne institucije i međunarodni partneri (OEBS, ENCYSEC, ICITAP, KEU, UNDP)	Broj održanih sastanaka
2.1.3	Izrada periodičnih izveštaja	Svaki 3 muaj	Planirani troškovi	Nacionalni koordinator	Relevantne institucije i međunarodni partneri	Broj sastavljenih izveštaja
2.1.4	Ponovno razmatranje Akcionog plana	K4 2016 K4 2017 K4 2018	Donacija (OEBS)	Nacionalni koordinator	Relevantne institucije i međunarodni partneri (OEBS, ENCYSEC,	Revidirani akcioni plan

					ICITAP, ZBE, UNDP)	
2.2	**Spečifični cilj: Izgradnja kapaciteta u sekretarijatu za strategije**					
Br.	**Aktivnosti**	**Rok**	**Budžet**	**Odgovorne institucije**	**Institucije koje podržavaju**	**Pokazatelji performanse**
2.2.1	Opis dužnosti i odgovornosti službenika odgovorni za sprovođenje Strategije kibernetičke bezbednosti	K1 2016	Administrativni troškovi	MUP	MJA, MF	Pozicija usvojena
2.2.2	Objavlivanje konkursa za zapošljavanje službenika odgovoran	K3 2016	Planirani troškovi	MUP	MJA, MF	Zaposleni službenik
2.3	**Spečivični cilj: Podizanje svesti**					
Br.	**Aktivnosti**	**Rok**	**Budžet**	**Odgovorne institucije**	**Institucije koje podržavaju**	**Pokazatelji performanse**
2.3.1	Objavljivanje biltena za kibernetičku bezbednost	2016-2019 .	Planirani troškovi	Nacionalni Koordinator	Relevantne institucije i međunarodni partneri (ICITAP, ENCYSEC, KEU, UNDP, OSBE)	Biletni objavljeni
2.3.2	Organizovanje kampanja za podizanje svesti	2016-2019	Donacija	Nacionalni Koordinator	Relevantne institucije i međunarodni partneri (ICITAP,	Broj organizovanih kampanja, predavanja održanih, podeljenih brošura,

					ENCYSEC, KEU, UNDP, OSBE)	
2.3.3	Dopunjavanje trenutnog nastavnog plana i programa TIK-a u pred - univerzitetskom nivou sa modulima kibernetičke bezbednosti	2016-2017	Administrativni troškovi	MONT	Nacionalni koordinator i Relevantne Institucije	Nastavni planovi dopunjeni
2.3.4	Organizozavnje Evropskog meseca za kibernetičku bezbednost	2016-2019	Donacija	Nacionalni Koordinator	Relevantne Institucije	Obeležavanje evropskog meseca za kibernetičku bezbednost
2.3.5	Organizovanje seminara i konferencija	2016-2019	Donacija (OEBS)	Nacionalni Koordinator	Relevantne institucije i međunarodni partneri (ICITAP, ENCYSEC, KEU, UNDP, OSBE)	Organizovane seminare i konferencije
2.3.6	Podizanje svesti i saradnje sa roditeljima, kao i organizovanje poseta i radionica za roditelje i decu o opasnostima od interneta	2016-2019	Administartivni troškovi	MONT	MKOS, MUP,NVO, međunarodni partneri	Organizovane radionice, posete u terenu
2.3.7	Uključivanje komponente za rizik koji dolazi iz interneta u nastavnim planovima i	2016	Administartivni troškovi	MONT	DKA	Nastavni planovi dopunjeni

	programima u preduniverzitetskom obrazovanju					
2.3.8	Podizanje svesti učenika kroz realizaciju nastavnih planova i programa koji se odnose na zaštitu od opasnosti inerneta	2016-2019	Administartivni troškovi	MONT	MONT, DKA, institucije visokog obrazovanja, Inspektorat za obrazovanje	Preduzete kampanje za podizanje svesti
2.3.9	Prprema plana progrma za predavanje i školskim institucijama u vezi sa zaštitom deca od interneta	2016-2019	Administartivni troškovi	MONT	MUP, PK, Relevantne institucije i međunarodni partneri	Nastavni plan i program, izrađen
2.3.10	Organizovanje aktivnosti za podizanje svesti o upotrebi bezbednog interneta od strane dece	2016-2019	Planirani troškovi	MONT	MONT, DKA, škole, međunarodni partneri	Organizirane aktivnosti
2.311	Izrada administrativnog upustva za upotrebu interneta u školi	2016-2017	Planirani troškovi	MONT	DKA, zajednica roditelja, međunarodni partneri	Administrativno upustvo usvojen i raspodela 12 000 priručnika
2.4	**Objektivi specifik: Pravna infrastruktura**					
Br.	Aktivnosti	Rok	Budžet	Odgovorne institucije	Institucije koje podržavaju	Pokazatelji performanse
2.4.1	Ponovno razmatranje Zakona	K1 2016	Administartivni troškovi	MER	Relevantne institucije	Izrađena procena

	za sprečavanje i borbu protiv kibernetičkog zločina k					
2.4.2	Razvoj politika i standardnih operativnih procedura (SOP) za odgovor na incidente sa računarima, kao i njihovu distribuciju u svakom relevantnom organizaciju koja se suočava sa velikim kibernetičkim pretnjama;	2016-2019	Administartivni troškovi	Nacionalni koordinator	Relevantne institucije	Izrađena PSO-
2.4.3	Izrada i usvojenje Pravilnika za tehničke zahteve koji garantuju bezbednost, integritet i poverenje	K4 2016	Administartivni troškovi	ROEPK	Cullen International, stručnjaci iz oblasti	Usvojeni pravilnik od strane borda RAEPK
2.4.4	Izrada i usvojenje zakona za identifikaciju i zaštitu kritične infrastrukture	K4 2016	Planirani troškovi	MUP	Relevantne institucije	Usvojeni zakon u Skupštini
2.5	**Spečifični cilj: Ljudski kapaciteti**					
Br.	**Aktivnosti**	**Rok**	**Budžet**	**Odgovorne institucije**	**Institucije koje podržavaju**	**Pokazatelji performanse**
2.5.1	Izrada planova i programa za obuku	2016-2019	Planirani troškovi	Nacionalni koordinator	Relevantne institucije, drugi	Broj izrađenih kurseva

					međunarodni partneri (USA amasada, ICITAP, UNDP, ENCYSEC, ZBE i OEBS)	
2.5.2	Obuka i sertifikacija osobalja za bezbednost tehnologije	2016-2019	Donacija	Nacionalni koordinator	Relevantne institucije, drugi međunarodni partneri (USA amasada, ICITAP, UNDP, ENCYSEC, ZBE i OEBS)	Broj obuka i serfikovanih službenika
2.5.3	Izrada scenaria i vežba za kibernetičku bezbednost	2016-2019	Administartivni troškovi	Relevantne institucije	Međunarodni Partneri (USA amasada, ICITAP, UNDP, ENCYSEC, ZBE i OEBS)	Broj izrađenih scenaria i realizovanih vežba
2.6	**Specifični cilj: Tehnička infrastruktura**					
Strateški cilj 3 Izgradnja javno- privatnog partnerstva						
3.1	**Spečifični cilj: Povečanje saradnje sa privatnim sektorom**					
Br.	**Aktivnosti**	**Rok**	**Budžet**	**Odgovorne institucije**	**Institucije koje podržavaju**	**Pokazatelji performanse**
3.1.1	Određivanje kontakt tačaka za sradnju sa privatnim sektorom	2016	Administartivni troškovi	Nacionalni koordinator	Privatni sektor	Određene kontakt tačke privatnog sektora
3.1.2	Saradnja sa pružiocima Internet usluga i komunikacija za	2016-2019	Administartivni troškovi	Nacionalni koordinator	Privatni sektor	Broj razmenjenih informacija

	identifikaciju i zaštitu od štetnog dejstva					
3.1.3	Stvaranje, u saradni sa privatnim sektorom, minimalnih kriterijumi obavezbe za zaštitu kritične infarstrukture informacije	2016	Planirani troškovi	Nacionalni koordinator	Privatni sektor	Izrađeni minimalni obavezni kriterijumi
3.1.4	Organizovanje redovnih sastanaka između javnog i privatnog sektora	2016-2019	Administartivni troškovi	Nacionalni koordinator	Privatni sektor	Broj održanih sastanaka
Strateški cilj 4 Odgovarajući na incidenata						
Strateški cilj 5 Međunarodna saradnja						
5.1	**Spečifični cilj: Organizacija i učešće u međunarodnim organizacijama**					
Br.	**Aktivnosti**	**Rok**	**Budžet**	**Odgovorne institucije**	**Institucije koje podržavaju**	**Pokazatelji performanse**
5.1.1	Organizacija međunarodnih aktivnosti za kibernetičku bezbednost godišnjih događaja	2016-2018	Donacija	Nacionalni koordinator	Relevantne institucije i međunarodni partneri (ICITAP, OEBS, ENCYSEC, KEU, UNDP)	Broj organizovanih aktivnosti
5.1.2	Učešće u međunarodnim	2016-2019	Donacija	Relevantne institucije	Nacionalni koordinator,	Broj aktivnosti i broj učesnika

	aktivnostima u oblasti kibernetičke bezbednosti				međunarodni partneri (ICITAP, OEBS, ENCYSEC, KEU, UNDP)	
5.2	**Specifični cilj: Jačanje međunarodne suradnje**					
Br.	**Aktivnosti**	**Rok**	**Budžet**	**Odgovorne institucije**	**Institucije koje podržavaju**	**Pokazatelji performanse**
5.2.1	Uspostavljanje partnerstva sa ENISA	2016-2019	Planirani troškovi	Nacionalni koordinator	MUP,MBSK, PK, ROEPK, DAI,	Broj poseta, učešća , vežbi i drugim aktivnostima u organizaciji ENISA
5.2.2	Unapređenje regionalne i međunarodne saradnje u borbi protiv kibernetičkog zločina	2016-2019	Administartivni troškovi	PK, KAI, CK, JFI, TSK, SSK	Relevantne institucije	Broj razmenjenih informacija, broj zajedničkih istraga, broj zajedničkih operacija
5.2.3	Osnivanje stalne kontakt tačke 24/7 za međunarodnu saradnju u oblasti borbe protiv kibernetičkog zločina	2016	Planirani troškovi	Nacionalni koordinator, MUP, PK	Relevantne institucije	Kontakt tačka 24/7 osnivana