CRNA GORA

STRATEGIJA

Podgorica, Jul 2013. godine

SADRŽAJ

1. UVOD

Informaciono komunikacione tehnologije predstavljaju nezamjenjiv dio savremenog života. Integracija ICT u obavljanju svakodnevnih aktivnosti i poslova postaje sve više evidentna, s tim u vezi prijetnje po informaciono komunikacionu infrastrukturu koje mogu da ugroze dostupnost, privatnost i integritet istih, takođe mogu da utiču na funkcionisanje društva kao cjeline.

Donošenje nacionalne sajber strategije predstavlja kompleksan zadatak imajući u vidu različite aspekte i aktere koji treba da budu uključeni u ovaj proces. Ovdje se može govoriti o političkom, zakonodavnom, ekonomskom, vojnom i sl. pogledu pri donošenju strategije, kao i o integraciji privatnog i javnog sektora kao vlasnika infrastrukture.

Strateški cilj Crne Gore je izgradnja integrisanog, funkcionalnog i efikasnog sajber prostora, a u skladu sa međunarodnim standardima i principima.

Svaka država je dužna da štiti svoju nacionalnu informatičku infrastrukturu, kao i svoj sajber prostor koji pokriva nacionalni domen.

Kako bi odgovorili na sajber prijetnje u okuženju koje se konstantno mijenjaju, države moraju imati fleksibilne i dinamične strategije sajber bezbjednosti. Prekogranična priroda prijetnji čini neophodnim da se države fokusiraju na jaku međunarodnu saradnju. Sveobuhvatne nacionalne strategije sajber bezbjednosti su prvi korak u tom pravcu.

Strategija treba da ima jasno definisane ciljeve i prioritete, a praksa je da oni budu definisani za razdoblje do 5 godina. Uz tekst Strategije koja predstavlja viziju određene zemlje a naspram pojma sajber bezbjednosti i garantovanja iste, definišu se i odgovarajući jednogodišnji akcioni planovi.

Internet, kao i informaciono komunikacione tehnologije na kojima je baziran, predstavljaju vitalni resurs za socio-ekonomski rast i razvoj jedne države. Kako se sve više usluga nudi putem interneta, sve je veći broj prijavljenih sajber bezbjednosnih incidenata, od napada poznatih kao distribuirani napadi uskraćivanja usluga – DDoS napadi, pa do napada na *web* sajtove sa ciljem neovlašćene izmjene njihovog sadržaja. Poseban vid opasnosti predstavlja i neautorizovan pristup razvijenim informacionim sistemima državnih organa, kao i njihovim bazama podataka. Internet servis provajderi (ISP) takođe trpe sajber napade na njihovoj infrastrukturi, ali ne postoji koordinisan odgovor, koji bi se odvijao bezbjednim komunikacionim kanalima na nacionalnom nivou u cilju rješavanja ovakvih situacija.

Jedan od problema predstavlja nedostatak neophodnih vještina za uspješnu odbranu od incidenata, kao i potreba za izmjenama i dopunama, ili donošenjem novih zakona, na osnovu

kojih bi bilo moguće uspješno otkrivati i krivično goniti lica koja se bave svim oblicima računarskog kriminala.

Još jedan značajan problem je taj da u Crnoj Gori ne postoji definisan način za praćenje ili evidenciju malicioznog saobraćaja koji ulazi u zemlju. Ne postoje adekvatni sistemi za monitoring postavljeni na komunikacionim čvorištima (*gateways*) prema inostranstvu ili na nivou ISP-a, izuzev za detekciju i sprečavanje napada usmjerenih ka uskraćivanju usluga (*DoS-DDoS*).

Koordinisana izgradnja organizacionih, insitucionalnih i upravljačkih kapaciteta, unapređenje zakonskih i podzakonskih propisa bitne su stavke postojanja informacione bezbjednosti u Crnoj Gori.

Prepoznajući svoje spoljnopolitičke prioritete kroz punopravno članstvo u NATO i EU, obezbjeđivanje propisanih bezbjednosnih kriterijuma na nacionalnom nivou postaje prioritet cjelokupnog informacionog društva Crne Gore.

Istovremeno, ekonomska i industrijska špijunaža usmjerena protiv vodećih kompanija i vlada takođe dobija na značaju sa razvojem i progresom u domenu informacionih tehnologija. Na kraju, nedozvoljeni ulaz, manipulacija podacima, kao i uništavanje kritičnih resursa takođe prijeti integrtitetu i otpornosti kritične infrastrukture.

U sajber prostoru, današnjicu obilježavaju i *"zlonamjerni programi u službi država"*, i u narednom periodu predstavljaće jednu od glavnih opasnosti po nacionalnu bezbjednost jedne države.

Gore navedeno govori u prilog činjenici da su Internet i sa njim povezane globalne mreže značajno uvećali svjetsku zavisnost od ICT i ujedno povećali nivo potencijalne štete koju je moguće prouzrokovati kada je infrastruktura pod napadom.

Strategija informacione bezbjednosti se oslanja na dokument koji je Vlada Crne Gore usvojila 2012. godine, pod nazivom ‘***'Elaborat sa definisanim nadležnostima državnih organa u borbi protiv sajber (računarskog) kriminala***''

S toga je donošenje Strategije sa jasnom vizijom na planu sprovođenja konkretnih aktivnosti u oblasti sajber bezbjednosti od ključnog značaja.

2. DEFINICIJE

Analizom strategija sajber bezbjednosti velikog broja država utvrđeno je da ne postoji usaglašena definicija pojmova kao što su: *informaciona bezbjednost*, *sajber prostor*, *sajber bezbjednost*, *sajber kriminal* i sl. Dok neke strategije definišu pomenute pojmove precizno i konkretno npr. usko vezujući ih za računare i računarske sisteme, druge imaju opštiji pristup i definicije sadrže ne samo stvari koje se odnose na računare i računarske sisteme već na bilo koji drugi faktor koji može doći u interakciju sa njima kao npr. ljudski faktor. U ovom poglavlju, biće prikazane definicije određenih termina, koje su zastupljene u našoj državi, a koje su takođe usaglašene sa osnovnim značenjima termina, u zemljama EU.

„Sajber“ se definiše kao: „sve što se odnosi na, ili uključuje, računare ili računarske mreže (kao što je Internet)“. **Sajber prostor** je više nego Internet, uključuje ne samo hardver, softver i informacione sisteme, već i ljude, društvenu interakciju u okviru ovih mreža. Međunarodna unija za telekomunikacije (ITU) koristi termin da opiše „sisteme i servise povezane bilo direktno ili indirektno na Internet, telekomunikacione sisteme ili kompjuterske mreže“. Međunarodna organizacija za standardizaciju (ISO) koristi nešto drugačiji termin pri definisanju, te „sajber“ vidi kao „kompleksno okruženje koje rezultira iz interakcije ljudi, softvera i servisa na internetu i to posredstvom tehnoloških uređaja i mreža sa njima povezanim koji ne postoji u bilo kom fizičkom obliku.“ Odvojeno, svaka država pri formulisanju nacionalne strategije koristi svoje termine i definicije. Primjer: Velika Britanija (UK) definiše sajber prostor kao „sve forme rada na mreži, digitalne aktivnosti; ovo uključuje sadržaj i akcije sprovedene kroz digitalne mreže“.

Informaciona bezbjednost podrazumijeva stanje povjerljivosti, cjelovitosti i dostupnosti podataka. Informaciona bezbjednost se fokusira na podatke bez obzira na njihovu formu: elektronski, štampani ili drugi oblici podataka.

Računarska bezbjednost obično teži da obezbijedi dostupnost i ispravno funkcionisanje računara i računarskog sistema.

Često dolazi do naizmjeničnog korištenja navedenih termina, i ako se odnose na malo drugačije aspekte u oblasti sajber bezbjednosti.

Internet bezbjednost u tehničkom kontekstu, se odnosi na „zaštitu Internet servisa i odnosnih ICT sistema i mreža kao produžetka mrežne bezbjednosti u organizacijama i domovima, a kako bi se obezbijedila svrha bezbjednosti. Internet bezbjednost takođe obezbjeđuje dostupnost i pouzdanost Internet servisa. Ipak, u političkom kontekstu, Internet bezbjednost se često izjednačava sa onim što je takođe poznato kao bezbjedno korišćenje

Interneta. Prema nekim definicijama, Internet bezbjednost podrazumijeva globalni režim koji se nosi sa stabilnošću Internet koda i hardvera, kao i sporazume o procesuiranju nelegalnog sadržaja. **Mrežna bezbjednost** je takođe važna za kritične infrastrukture koje često nisu direktno povezane na Internet.

Sajber bezbjednost - Međunarodna organizacija za standardizaciju (ISO) definiše sajber bezbjednost kao „očuvanje povjerljivosti, integriteta i dostupnosti informacija u sajber prostoru". Holandija je ponudila nešto širu definiciju: „sloboda od opasnosti ili štete prozrokovane prekidom, kvarom ili zloupotrebom rada ICT-a. Opasnost ili šteta prouzrokovana prekidom, kvarom ili zloupotrebom može se sastojati od ograničenja dostupnosti ili pouzdanosti ICT-a, kršenja privatnosti informacija sačuvanih na ICT uređajima, ili šteta integritetu informacija. ITU takođe definiše široko sajber bezbjednost kao: „Kolekcija alata, pravilnika, sigurnosnih koncepata, zaštita, smjernica, pristupa u upravljanju rizicima, akcija, obuka, najboljih praksi, uvjerenja i tehnologija koje se mogu koristiti radi zaštite sajber okruženja i organizacija i korisničke imovine. Sajber bezbjednost pretenduje da obezbijedi postizanje i održavanje bezbjednosti imovine organizacije i korisnika protiv relevantnih sigurnosnih rizika u sajber okruženju. Generalni bezbjednosni ciljevi se sastoje od sljedećeg: dostupnosti; integriteta, koji može uključiti autentičnost i neporečivost; i povjerljivosti. "

Sajber odbrana se uglavnom koristi u vojnom kontekstu, ali može se odnositi i na kriminalne i špijunske aktivnosti.

NATO koristi sljedeću definiciju kada je riječ o sajber odbrani: „sposobnost da se osigura dostava i upravljanje servisima u operativnim komunikacionim i informacionim sistemima kao odgovor na potencijalne, neposredne kao i stvarne maliciozne akcije koje potiču iz sajber prostora".

Sajber kriminal - ili e-kriminal, ili VTK obuhvata kriminalne aktivnosti u kojima su kompjuteri i slični informatički uređaji i kompjuterska mreža predmet, sredstvo, cilj ili mjesto krivičnog djela.

Sajber prostor je prepoznat kao okruženje sa najbržim rastom stepena kriminala. Tokom poslednje decenije većina država je prepoznala problem sajber kriminala i sa tim u vezi donešeni su i usvojeni adekvatni zakoni. Kina je 1997. godine prepoznala kao nezakonitu aktivnost „upad u kompjutersko informacioni sistem", Savjet Evrope je 2004. godine usvojio Konvenciju o sajber kriminalu koja sadrži relativno visoke standarde na polju međunarodne saradnje, a u cilju procesuiranja sajber kriminala, ista je potpisana od strane 51 države.

Procjenjuje se da se tokom 2011. godine pojavilo više od 400 miliona različitih varijanti virusa i u prosjeku 8 novih „zero day" eksploatacija na dnevnom nivou. Ovaj podatak predstavlja alarmantnu činjenicu. Kako se granice legalnog procesuiranja poklapaju sa granicama različitih država prepoznata je snažna potreba za bliskom međunarodnom saradnjom.

Sajber terorizam – predstavlja kriminalni akt u sajber prostoru koji ima za cilj da se zaplaši vlada iili njeni građani, a sve u cilju ostvarivanja političkih ciljeva. NIPC (National Infrastructure Protection Center) definiše sajber terorizam kao „kriminalni akt izvršen putem računara, a koji za rezultat ima nasilje, smrt i/ili destrukciju, stvarajući teror radi ubjeđivanja vlade da promijeni svoju politiku".

Sajber špijunaža je definisana kao, „korišćenje agenta u cilju dobijanja informacija u vezi sa planovima ili aktivnostima strane države ili konkurentske kompanije". Nije rijedak slučaj gdje su kompanije ili vlade suočene sa pokušajima neautorizovanih pristupa njihovim kompjuterskim sistemima putem Interneta. Mnoge države koriste sredstva špijunaže da bi podstakli svoj ekonomski razvoj baziran na naprednim tehnologijama drugih nacija. ICT predstavlja bazičnu osnovu u razvoju i implementaciji većine drugih tehnologija kako u civilnom tako i u vojnom sektoru, i usled toga postale su primarni cilj špijunaže.

Sajber ratovanje je neodređen i kontroverzan termin za koji ne postoji zvanična ili generalno prihvaćena definicija. Više od 30 država je prihvatilo doktrinu i najavilo razvoj specijalnog programa ofanzivnih mehanizama sajber ratovanja.

3. UPRAVLJANJE SISTEMOM SAJBER BEZBJEDNOSTI

Jedna od ključnih preporuka međunarodnih subjekata (NATO, ENISA) je da strategiju treba razvijati u okviru životnog ciklusa koji treba da sadrži sledeće faze:

1. Razvoj,
2. Implementacija,
3. Evaluacija i
4. Prilagođavanje strategije.

Na ovaj način obezbijediće se kontinuirani progres strategije, procedura i proizvoda, a u skladu sa izmijenjenim okolnostima u neposrednom i širem okruženju.

Javno tijelo ili interna radna grupa ili Savjet na ***nacionalnom*** nivou, treba da se definiše kao koordinator realizacije strategije, te isto treba da bude odgovorno za monitoring cjelokupnog životnog ciklusa strategije. Pozitivna praksa je da članovi ovog tijela sa jedne strane budu lica sa visokom javnom ili privatnom funkcijom, a sa druge strane da imaju napredno znanje iz oblasti sajber zaštite i bezbjednosti, kako bi imali dovoljan kredibilitet i efikasnije obezbjedili ostvarivanje prepoznatih strateških ciljeva.

Uspješna implementacija strategije o sajber bezbjednosti zahtjeva adekvatnu i kontinuiranu saradnju javnog i privatnog sektora, tj. zainteresovanih strana iz jednog i drugog sektora. Izabrana privatna tijela treba da budu dio razvojnog i implementacionog procesa zbog vjerovatnoće da su upravo oni vlasnici kritične informacione infrastrukture i servisa.

Razvoj i planiranje nacionalnog sajber kriznog plana predstavlja bitan faktor u generalnom planiranju sajber bezbjednosti jedne države. On treba da bude realan i precizan a takođe u njemu treba da budu uzeti u obzir svi mogući učesnici.Ovo podrazumjeva interakciju javnog i privatnog sektora.

Strategija svakako treba da obuhvata procjenu nacionalnih rizika, koja mora biti realna, a u cilju što efikasnijeg sprovođenja strategije. Prilikom procjene neophodno je imati usaglašenu metodologiju, kao i pristup koji bi obezbjedio da se razmotre sve moguće prijetnje i opasnosti koje postoje.

Bitan dio ovog procesa predstavlja prepoznavanje i definisanje kritične nacionalne infrastrukture, prijetnji i rizika po nju. Posljednji treba da budu klasifikovani po stepenu njihovog uticaja, odnosno posljedica koje bi prouzrokovali, kao i po procjeni vjerovatnoće njihovog realnog dešavanja.

3.1 NAČIN PRAĆENJA ŽIVOTNOG CIKLUSA STRATEGIJE

Pored konstantnog zalaganja da strategija mora da prati odgovarajući životni ciklus, ovdje se ukazuje i na više konkrektnih aktivnosti koje donosioci odluka treba da realizuju:

- Postaviti viziju, opseg, ciljeve i prioritete;
- Pratiti procjene rizika na nacionalnom nivou;
- Uzeti u obzir postojeće politike, regulative i kapacitete;
- Razviti jasnu upravljačku strukturu;
- Identifikovati i uključiti zainteresovane strane;
- Uspostaviti povjerljive mehanizme razmjene informacija;
- Razviti sajber bezbjednosne planove za nepredviđene slučajeve;
- Organizovati sajber bezbjednosne vježbe;
- Uspostaviti osnovne bezbjednosne zahtjeve;
- Uspostaviti mehanizme izvještavanja o incidentima;
- Povećati svijest građana o ovom pitanju;
- Njegovati ciklus istraživanja i razvoja;
- Jačati obuke i programe usavršavanja;
- Uspostaviti sposobnost odgovora na incidente;

- Odgovoriti na sajber kriminal;
- Uključiti se u međunarodnu saradnju;
- Uspostaviti javno-privatna partnerstva;
- Balansirati između bezbjednosti i poštovanja privatnosti;
- Sprovoditi evaluacije;
- Usklađivati nacionalnu strategiju o sajber bezbjednosti.

3.2 IZAZOVI, RIZICI I PRIJETNJE PO BEZBJEDNOST SAJBER PROSTORA U CRNOJ GORI

Istraživanjem o upotrebi informaciono-komunikacionih tehnologija u Crnoj Gori koje je sproveo Zavod za statistiku Crne Gore 2012.godine, dobijeni su sljedeći rezultati:

Domaćinstva:

- 51,3% ima pristup personalnom računaru (PC),
- 33,6% domaćinstava koristi laptop
- 93,3% ima mobilni telefon.

U Crnoj Gori, 55,0% anketiranih domaćinstava je izjavilo da ima pristup Internetu kod kuće. Pristup Internetu se pri tom ostvaruje pomoću nekog od uređaja, kao što su personalni računar (PC) –75,3% domaćinstava i laptop –52,0%. Pored navedenih uređaja za pristup Internetu se koriste i mobilni telefoni- 24,2%, ručni računari (palmtop, PDA, tablet), igračke konzole (play station) itd.

Na pitanje "Da li ste u posljednjih 12 mjeseci naišli na bilo koji od navedenih problema u vezi sa bezbjednošću prilikom upotrebe Interneta u privatne svrhe?", građani su odgovorili na sljedeći način:

Na pitanje da li koriste IT bezbjednosne softvere u cilju zaštite svog privatnog računara i podataka na njemu (antivirus, antispam, firewall itd.), dobijeni su sljedeći rezultati:

Privredni subjekti:

U Crnoj Gori 88,3% anketiranih preduzeća je izjavilo da je koristilo računare u svom poslovanju tokom januara 2012. godine.

Prema rezultatima istraživanja 53,3% preduzeća (koja su koristila računar u svom poslovanju) je svojim zaposlenim omogućavalo daljinski pristup e-mail sistemu, dokumentima ili aplikacijama preduzeća, tokom januara 2012. godine.

Kada je riječ o Internetu, istraživanje je pokazalo da je 96,1% preduzeća, koja su koristila računar, imalo pristup Internetu, tokom januara 2012. godine. Ovo predstavlja rast od 1% u odnosu na prethodnu godinu. Od preduzeća koja su imala pristup Internetu, 53,1% je odgovorilo da su imala Web Site/Home Page, tokom januara 2012. godine.

Na pitanje o zapošljavanju IT stručnjaka tokom januara 2012. godine, samo je 20,8% preduzeća odgovorilo da je zapošljavalo stručnjake kojima je IT glavni posao.

U Crnoj Gori samo 27,9% preduzeća posjeduje pravilnik kojim su normativno regulisana pitanja informacione bezbjednosti. Takođe je veoma mali procenat preduzeća koja vrše provjeru zaposlenih o poznavanju mjera informacione bezbjednosti, svega 26,9% preduzeća.

Ključni rizici, izazovi i prijetnje po sajber bezbjednost u Crnoj Gori su:

a. Propusti u organizaciji sajber zaštite mogu predstavljati opasnost po nacionalnu bezbjednost Crne Gore;

b. Internet se u Evropi pa i u našem bliskom okruženju intenzivno koristi u kriminalne svrhe, za potrebe trgovine drogom, pranja novca i finansijskih prevara, pa ni Crna Gora nije i neće biti pošteđena ove opasnosti;

c. ICT infrastruktura, računarski sistemi i korisnici u Crnoj Gori izloženi su većini sajber opasnosti i napada koje su pogađaju ostatak svijeta. Ovo uključuje maliciozne programe, elektkronske prevare, izmjene naslovnih web stranica (Web Defacement) i "hakovanje" elektronske pošte;

d. Nerazvijena saradnja između privatnog i javnog sektora u oblasti koordinacije sistema bezbjednosti kritične infrastrukture;

e. Nepostojanje procedure evidencije incidentnih situacija u sajber prostoru Crne Gore

f. Nepostojanje Nacionalnog savjeta za sajber bezbjednost sa njegovim funkcijama:

    i. Koordinacija informacione bezbjednosti u Crnoj Gori

    ii. Definisanje kritične informatičke infrastrukture

    iii. Razmatranje legislativnog okvira za razvoj operativne sajber bezbjednosti.

g. Sajber prostor se sve više koristi za organizaciju i medijsku propagandu ekstremističkih i radikalnih grupa koje na taj način propagiraju svoje aktivnosti, vrbuju nove članove, organizuju terorističke akcije i tako predstavljaju opasnost po nacionalnu bezbjednost Crne Gore.

h. Piraterija doprinosi visokoj stopi zaraženosti računarskim virusima.

i. On-line manipulacije, koristeći socijalni inženjering putem e-mail poruka, kao što je *„Nigerian 419"* prevara, *phishing*, idu ruku pod ruku sa krađom identiteta (nezakonita saznanja o nalozima i lozinkama drugih korisnika). Ovakvo stanje u crnogorskom sajber-prostoru je zabrinjavajuće i problematično i ne samo za Crnu Goru već i šire. Crnogorski građani u

prošlosti su bili mete prevara i u tim prevarama čak ostajali i bez veće sume novca;

j. U periodu od 2008.-2013. godine, napadači su izmijenili ili preuzeli kontrolu nad više naslovnih web stranica crnogorskih institucija;

k. U Crnoj Gori je u prošlom periodu bilo više napada na informatičku infrastrukturu, na servise provajdera interneta kao i na bankarski sektor;

l. Prethodnih godina je primijećen i značajan broj slučajeva u kojima su napadači preuzeli kontrolu nad korisničkim profilima crnogorskih državljana na društvenim mrežama i ostavljali u ime vlasnika neprimjereni sadržaj, sve u cilju kompromitovanja vlasnika profila.

m. Sa adresa, za koje se istragom utvrdilo da potiču iz Crne Gore, prijavljeno je maliciozno djelovanje, između ostalog širenja SPAM-a, napadi probijanja lozinke metodom sile (brute force), DDoS napadi, lažno predstavljanje i drugi;

n. U Crnoj Gori, postoji vrlo mali broj kadrova koji posjeduju usko specijalizovana znanja iz oblasti sajber bezbjednosti, tj. da posjeduju određene licence ili sertifikate iz ove oblasti, koje zahtijevaju evropski i svjetski standardi. U okviru Univerziteta u Crnoj Gori, ne postoje fakulteti ili smjerovi koji obrađuju sajber bezbjednost ili forenziku, tj. da proizvode kadrove sa usko specijalizovanim znanjem iz ove oblasti.

4. INSTITUCIONALNI I PRAVNI OKVIR CRNE GORE

4.1. Analiza pravne regulative Crne Gore i EU

Crna Gora je odgovarajući zakonski i pravni okvir koji pravno onemogućava svaki vid slučajnog ili namjernog narušavanja i sprečavanja funkcionisanja informatičkog sistema započela da izgrađuje u poslednjih nekoliko godina kroz reforme krivičnog zakonodavstva. Odgovarajući zakonski okvir predstavlja sponu pravne i informacione oblasti, koja će zajedničkom saradnjom doprinijeti uspješnom rasvjetljavanju slučaja iz oblasti računarskog kriminala i sankcionisanja počinilaca.

Regionalnu Deklaraciju o strateškim prioritetima u borbi protiv računarskog kriminala Crna Gora je potpisala u Dubrovniku 15. februara 2013. godine, u kojoj su prepoznati strateški prioriteti u borbi protiv računarskog kriminala koje ova Strategija prati i dalje razvija.

Evropska konvencija iz 1959. godine o pružanju međusobne pravne pomoći u krivičnim stvarima predstavlja preteču Konvencije o sajber kriminalu koja je donijeta da bi poslužila kao okvir državama koje žele da pravno kodifikuju ovu vrstu društveno opasnog ponašanja.

Konvencija o sajber kriminalu ili u medjunarodnoj zajednici poznata kao Budimpeštanska konvencija donijeta je 21.11.2001. godine od strane Savjeta Evrope, a na snazi je od jula 2004. godine.

Konvenciju je potpisala 51 država, od kojih 6 država nisu članice Savjeta Evrope, a to su Australija, Dominikanska Republika, Kanada, Japan, Južna Afrika i SAD.

Ova Konvencija spada u krug okvirnih konvencija, što znači da njene odredbe nisu direktno primjenjive, već da je neophodno da ih države implementiraju kroz svoje vlastito odnosno nacionalno zakonodavstvo.

Crna Gora je donijela Zakon o potvrđivanju Konvencije o računarskom kriminalu 3. marta 2010. godine, koji je stupio na snagu 1. jula 2010. Takođe Crna Gora je ratifikovala i Dodatni protokol o rasizmu i ksenofobiji (CETS 189) zajedno sa Konvencijom 3. marta 2010., koji je stupio na snagu 1. jula 2010. Crna Gora je potpisala i ratifikovala Konvenciju o Zaštiti djece protiv seksualne ekploatacije i seksualnog zlostavljanja (CETS 201).

Krivična djela koja su predviđena ovom Konvencijom kao sajber kriminal obuhvataju široku lepezu od širenja virusa, neovlašćenog pristupa računarskoj mreži preko piraterije do pornografije i upada u bankarske sisteme, zloupotrebe platnih kartica ali i svih ostalih krivičnih djela u kojima se koriste kompjuteri. Crnogorsko krivično zakonodavstvo usaglašeno je sa odredbama Budimpeštanske konvencije.

Budimpeštanska konvencija predviđa da nacionalna zakonodavstva u svojim krivičnim zakonima predvide kažnjivost djela koja se odnose na kršenje autorskih i njima sličnih prava, i obavezama koje su preuzete iz Konvencije iz Berna o zaštiti književnih i umjetničkih djela, zaštiti po ugovoru o komercijalnim aspektima prava na intelektualnu svojinu i Svjetska organizacija intelektualne svojine (WIPO) ugovorom o autorskim pravima. Kodifikaciju ovih krivičnih djela naš Krivični zakonik je dao u odredbama koje se odnose na povredu moralnih prava autora i interpretatora, neovlašćeno iskorišćavanje autorskog djela ili predmeta, neovlašćeno zaobilaženje mjera zaštite namijenjenih sprečavanju povreda autorskog i srodnih prava, neovlašćeno uklanjanje ili mijenjanje elektronske informacije o autorskom i

srodnom pravu, neovlašćeno korišćenje tudjeg patenta i neovlašćeno korišćenje tuđeg dizajna.

Konvencija takođe predviđa odgovornost pravnih lica, a kada to pretočimo u naše nacionalno zakonodavstvo onda možemo reći da je Crna Gora 2007. godine donijela Zakon o odgovornosti pravnih lica za krivična djela pa je svojim članom 3 predvidjela da pravna lica mogu da odgovaraju za sva krivična djela iz posebnog dijela krivičnog zakonika, kao i za sva druga krivična djela koja su propisana posebnim zakonom uz uslov da su ispunjeni uslovi za odgovornost pravnog lica koje propisuje Zakon o odgovornosti pravnih lica za krivična djela.

Crna Gora je ratifikovala dodatni Protokol uz konvenciju o računarskom kriminalu, a ovaj **Dodatni protokol govori o kažnjavanju akata rasizma i ksenofobije koji su učinjeni putem računarskih sistema**. Ovaj Protokol je ratifikovan 03.03.2010. godine a stupio je na snagu 01.07.2010. godine. Ovaj Protokol implementiran je kao poseban član Krivičnog zakonika koji govori o izazivanju nacionalne, rasne i vjerske mržnje.

Okvirna odluka Vijeća EU 2005/222/PUP odnosno Eurlex broj 32005F0222 govori o napadima na informacione sisteme i ona je implemetirana kroz odredbe Krivičnog zakonika.

Takođe veoma značajan međunarodni izvor prava je i **Okvirna odluka vijeća EU 32000D0375** koja je donijeta 29.05.2000. godine i govori o suzbijanju dječije pornografije na internetu, i predviđa niz konkretnih mjera o cilju prevencije i suzbijanju proizvodnje obrade, posjedovanja i distribucije materijala sa dječijom pornografijom i o cilju efikasnosti istraga i krivičnog progona za prestupe iz ove oblasti. Zakonik o krivičnom postupku Crne Gore predviđa mjere za koje možemo reći da su djelimično usaglašene sa ovom okvirnom odlukom, a u pitanju su hitnost postupka kada su ova djela u pitanju, isključenje javnosti za ova djela, s tim što su ovo opšte odredbe koje se tiču postupaka u vezi sa maloljetnicima.

Procesno pravo

Konvencija o sajber kriminalu govori i o procesnim odredbama za oblast sajber kriminala. Konvencija preporučuje državama potpisnicama da u svojim nacionalnim zakonodavstvima usvoji sve zakonske i ostale neophodne mjere kako bi se uspostavila određena ovlašćenja i procedure za kažnjivost krivičnih djela iz oblasti sajber kriminala.

Crna Gora je donijela novi Zakonik o krivičnom postupku koji je u skladu sa međunarodnim pravnim standardima i potpuno ili djelimično uskladila domaće procesne norme sa određenim procesnim odredbama koje propisuje Konvencija iz Budimpešte, kao što su članovi Konvencije koji se odnose na radnje dokazivanja, mjere tajnog nadzora i privremeno oduzimanje predmeta i imovinske koristi implementirani su u naš Zakonik o krivičnom postupku.

Zakonodavni okvir

Pravni akti koji čine temelj funkcionisanja i osnov za dalju nadogradnju savremenog koncepta informacione bezbjednosti u Crnoj Gori:

a) **Zakon o potvrđivanju konvencije o računarskom kriminalu**

b) **Krivični zakonik**

c) **Zakonik o krivičnom postupku**

d) **Zakon o informacionoj bezbjednosti**

e) **Zakon o Agenciji za nacionalnu bezbjednost**

f) **Zakon o tajnosti podataka**

g) **Zakon o elektronskom potpisu**

h) **Zakon o elektronskim komunikacijama**

i) **Zakon o elektronskoj trgovini**

Ostali važni akti koje treba pomenuti u ovom poglavlju:

- Elaborat sa definisanim nadležnostima državnih organa u borbi protiv računarskog kriminala kojim je izvršena procjena stanja i spremnosti države u oblasti sajber bezbjednosti
- Uredba o bližim uslovima i načinu sprovođenja informatičkih mjera zaštite tajnih podataka (01.jul 2010.godine)
- Uredba o bližim uslovima i načinu sprovođenja mjera zaštite tajnih podataka (06.novembar 2008. godine)
- Uredba o bližim uslovima i načinu sprovođenja industrijskih mjera zaštite tajnih podataka (16.decembar 2010. godine)
- Uredba o načinu vršenja i sadržaju unutrašnje kontrole nad sprovođenjem mjera zaštite tajnih podataka (28. jul 2010. godine).

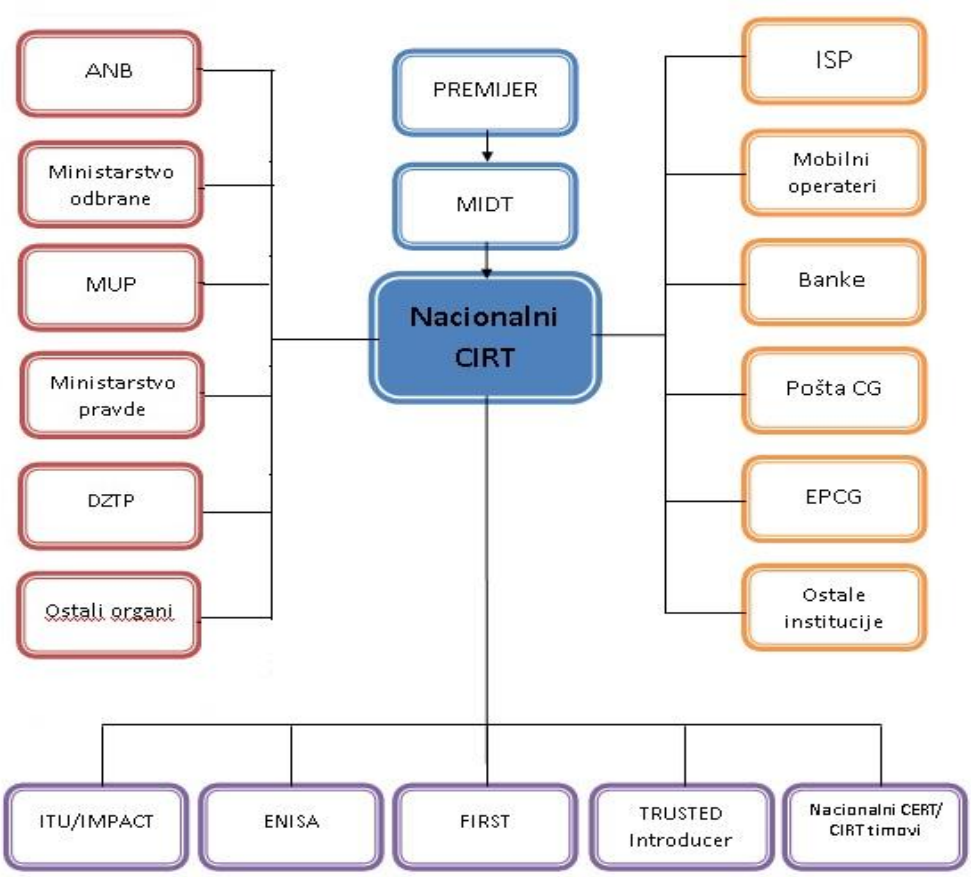
4.2. Nosioci sistema sajber bezbjednosti Crne Gore

U okviru državne uprave neophodno je da postoji definisana organizaciona hijerarhija koja će najefikasnije i dugoročno održivo obezbjeđivati adekvatno upravljanje informacionom bezbjednošću u Crnoj Gori.

U Crnoj Gori su prepoznate sljedeće institucije koje su ključne na polju sajber bezbjednosti:

- Ministarstvo za informaciono društvo i telekomunikacije (Nacionalni CIRT)
- Ministarstvo odbrane
- Ministarstvo unutrašnjih poslova
- Ministarstvo pravde
- Agencija za nacionalnu bezbjednost
- Uprava policije
- Vojska Crne Gore
- Direkcija za zaštitu tajnih podataka
- Univerziteti u Crnoj Gori

Nacionalni CIRT predstavlja centralno mjesto za koordinaciju i razmjenu podataka, odbranu od sajber napada i otklanjanje posledica sajber bezbjednosnih incidenata za područje Crne Gore.



Slika 1: Pozicija Nacionalnog CIRT-a u sistemu sajber bezbjednosti u Crnoj Gori

Članovi ove hijerarhijske infrastrukture su i CIRT-ovi ili slična organizaciona tijela koja uspostavljaju Internet provajderi (ISP), mobilni operateri, banke, Pošta Crne Gore, EPCG i druge kompanije koje imaju interes ili značajan uticaj na funkcionisanje nacionalne informatičke infrastrukture.

CIRT je postao član ključnih međunarodnih institucija koje su relevantne na polju sajber bezbjednosti, kao što su FIRST (*Forum of Incident Response Security Teams*), TRUSTED Introducer (TERENA), ITU-IMPACT koalicija. Članstvom u ove organizacije, CIRT ostvaruje vezu sa drugim CERT/CIRT timovima iz cijelog svijeta.

5. GLAVNI CILJEVI STRATEGIJE SAJBER BEZBJEDNOSTI CRNE GORE

Strategija sajber bezbjednosti Crne Gore sadrži sedam ključnih oblasti:

1) Definisanje institucionalne i organizacione strukture na polju sajber bezbjednosti u državi

Koordinisana izgradnja organizacionih, insitucionalnih i upravljačkih kapaciteta, unapređenje zakonskih i podzakonskih propisa bitne su stavke postojanja informacione bezbjednosti u Crnoj Gori.

Formiranjem Nacionalnog Savjeta za sajber bezbjednost, dobija se krovna organizacija u državi koja će savjetovati Vladu Crne Gore o svim bitnim pitanjima koja se tiču sajber bezbjednosti. Savjet će predlagati mjere za usklađivanje zakonodavnog i administrativnog okvira u cilju efikasnije borbe protiv računarskog kriminala.

Članovi Savjeta su predstavnici ključnih institucija koje su prepoznate u borbi protiv računarskog kriminala.

Ključne aktivnosti:

- Osnivanje Nacionalnog Savjeta za sajber bezbjednost
- Formiranje lokalnih CIRT timova

2) Zaštita kritične informatičke infrastrukture u Crnoj Gori

Zbog konstantnog rasta broja usluga koje državni organi i privatni sektor pružaju, kako građanima tako i drugim pravnim subjektima, potrebno je definisati kritičnu informatičku infrastrukturu u Crnoj Gori i razviti procedure zaštite.

Neophodno je obezbijediti nacionalnu sajber bezbjednost i zaštititi ekonomske interese. S toga, Vlada mora obezbijediti neophodnu strukturu i resurse kako bi se osigurala sajber bezbjednost.

Ključne aktivnosti:

- Definisanje i zaštita kritične informatičke infrastrukture
- Jačanje otpornosti informacionih sistema na incidente
- Izvršiti analizu prijetnji za informatičku infrastrukturu

3) Jačanje kapaciteta državnih organa za sprovođenje zakona

Konstantno usavršavanje nivoa sofisticiranosti sajber prijetnji i napada kao i metoda i tehnika istih zahtijeva i kontinuirano jačanje administativnih kapaciteta jedne države a u cilju efikasnog odgovora na širok dijapazon sajber prijetnji.

Računarski kriminal (Sajber kriminal) i elektronski dokazni materijal zahtijevaju specijalizovani odgovor organa krivičnog pravosuđa. Organi za sprovođenje zakona i tužilaštvo treba da su u mogućnosti da sprovode istrage i procesuiraju djela protiv kompjuterskih podataka i sistema, djela koja se vrše pomoću kompjutera, kao i elektronski dokazni materijal koji se odnosi na bilo koje krivično djelo.

Ključne aktivnosti:

- Usvajanje potpunih i djelotvornih zakonodavnih rešenja u oblasti sajber kriminala, koji zadovoljavaju zahtjeve u oblasti ljudskih prava i vladavine prava
- Jačanje specijalizovane jedinice za borbu protiv računarskog kriminala u okviru Uprave policije
- Jačanje specijalizovane jedinice za borbu protiv računarskog kriminala u okviru Vojske Crne Gore
- Jačanje kapaciteta Agencije za nacionalnu bezbjednost u oblasti prikupljanja, evidentiranja, analize, čuvanja i razmjene podataka iz sajber prostora, a u skladu sa Zakonom o Agenciji za nacionalnu bezbjednost.
- Unaprijediti kapacitete za digitalnu forenziku

- Jačanje kapaciteta tužilaštva u oblasti računarskog kriminala i elektronskog dokaznog materijala
- Podržavanje obuka sudija, tužilaca i organa za sprovođenje zakona u oblasti računarskog kriminala
- Promovisanje finansijskih istraga i sprečavanje prevara i pranja novca na Internetu

4) Odgovor na incidentne situacije

Osnivanjem Nacionalnog CIRT-a pri Ministarstvu za informaciono društvo i telekomunikacije, napravljen je krupan korak ka sprečavanju i uklanjanju sajber prijetnji koje pogađaju državu i njene građanje. CIRT se u saradnji sa ključnim institucijama u CG bavi detekcijom, praćenjem i suzbijanjem sajber napada i sajber kriminalom na nivou države. CIRT predstavlja centralno mjesto za koordinaciju prevencije i zaštite od računarskih bezbjednosnih incidenata na Internetu i drugih rizika bezbjednosti informacionih sistema za područje Crne Gore. Omogućena je i prijava incidenata na portalu www.cirt.me.

Kako bi na što bolji i efikasniji način odgovorili na incidentne situacije, neophodno je obezbijediti kvalitetniju saradnju i nesmetanu razmjenu informacija između ključnih institucija na polju sajber bezbjednosti. Ovo se prvenstveno odnosi na saradnju ključnih državnih institucija sa ključnim institucijama iz privatnog sektora (Internet provajderi, agent za .me domen, mobilni operatori, bankarski sektor, elektroprivreda, pošta,..itd.).

Takođe, imajući u vidu da sajber napadi ne znaju za granice i da veliki broj sajber napada dolazi iz drugih zemalja, neophodno je uspostaviti i održavati saradnju sa relevantnim međunarodnim institucijama (FIRST, Trusted Introducer, ITU-IMPACT, itd.) i nacionalnim CERT/CIRT timovima drugih zemalja.

Ključne aktivnosti:

- Obezbijediti preko Nacionalnog Savjeta za sajber bezbjednost, proceduru za razmjenu informacija između državnih organa i organa uprave
- Obezbijediti obuke za zaposlene koji rade na polju sajber bezbjednosti u okviru CIRT-a
- Unaprijediti saradnju sa ključnim institucijama iz privatnog sektora.

- Nastaviti sa aktivnostima na saradnji nacionalnog CIRT-a Crne Gore sa ključnim međunarodnim organizacijama i CERT/CIRT timovima drugih zemalja.

5) Uloga Ministarstva odbrane i Vojske Crne Gore u sajber prostoru

Imajući u vidu sve veću ulogu informacionih tehnologija u vojnim operacijama, kao i potrebu da se zaštitimo od malicioznog sajber djelovanja, potrebno je razmotriti ulogu Ministarstva odbrane i Vojske Crne Gore u zaštiti sajber prostora Crne Gore. Uticaj sajber-bezbjednosti u vojnom domenu se razlikuje od zemlje do zemlje, kao što se i definicija vojnih sajber operacija isto razlikuje.

Prema nekim izvještajima NATO-a, oko 120 zemalja razvija vojne sajber kapacitete.

Ključne aktivnosti:

- Definisati ulogu Ministarstva odbrane i Vojske Crne Gore u sajber prostoru Crne Gore
- Jačanje kapaciteta Ministarstva odbrane i Vojske Crne Gore u oblasti sajber odbrane
- Uspostaviti saradnju na ovom polju sa internacionalnim partnerima.

6) Javno-privatno partnerstvo

Veliki dio kritične informatičke infrastrukture pripada privatnom sektoru. Zato je neophodno definisati jasnu saradnju sa privatnim sektorom na polju sajber bezbjednosti. Posebno definisati procedure o razmjeni informacija sa:

- Internet provajderima
- Agentom za .me domen
- Bankarskim sektorom
- Elektroprivredom
- Kompanijama koje hostuju e-servise u Crnoj Gori

7) Podizanje nivoa svijesti u društvu i zaštita na Internetu

Obezbijediti sigurnije internet okruženje za stanovnike Crne Gore i osposobljavanje korisnika kroz jačanje svijesti o potrebi obuke. Poseban fokus bi trebalo dati novim generacijama, kao krajnjim korisnicima Interneta i u kontinuitetu uvoditi nove programe o informacionoj bezbjednosti za sve nivoe obrazovanja u cilju korišćenja razvijenih informacionih sistema.

Ključne aktivnosti:

- Organizovati projekte i kampanje za promovisanje sigurnog korišćenja Interneta sa posebnim fokusom na zaštitu djece na internetu
- U saradnji sa Ministarstvom prosvjete i Univerzitetima u Crnoj Gori raditi na organizovanju posebnih programa iz oblasti sajber bezbjednosti sa ciljem stvaranja kadrova sa usko specijalizovanim znanjem iz ove oblasti
- Djelotvorna regionalna i međunarodna saradnja.

PRILOG I: AKCIONI PLAN ZA IMPLEMENTACIJU STRATEGIJE 2013-2015

BR	ZADATAK	OPIS	ODGOVORNI ORGAN	ROK
1	Osnivanje Nacionalnog Savjeta za sajber bezbjednost (informaciona bezbjednost)	Članovi Savjeta su predstavnici institucija koje su prepoznate kao ključne u oblasti sajber bezbjednosti. Članove Savjeta će imenovati Vlada Crne Gore na preporuku MIDT. U nadležnosti Savjeta će biti aktivnosti iz domena sajber bezbjednosti i INFOSEC-a.	MIDT	Decembar 2013.
2	Formiranje lokalnih CIRT timova u ključnim institucijama za borbu protiv sajber kriminala u cilju uspostavljanja Nacionalne CIRT infrastrukture	Svi državni organi i organi uprave, koji vode baze podataka od nacionalnog značaja ili upravljaju dijelom kritične informatičke infrastrukture, treba da formiraju lokalne CIRT timove.	MIDT	Mart 2014 .
3	Definisanje i zaštita kritične informatičke infrastrukture	Definisati Metodologiju koja će se koristiti za potrebe identifikovanja kritične informatičke infrastrukture. Neophodno je definisati kritičnu informatičku infrastrukturu u Crnoj Gori i razviti procedure za zaštitu kako bi se osiguralo njeno neometano funkcionisanje.	MIDT MO MUP ANB	Septembar 2014.
4	Unaprijediti saradnju između državnih organa i organa uprave	Obezbijediti preko Nacionalnog Savjeta za sajber bezbjednost, proceduru za razmjenu informacija između državnih organa i organa uprave.		Maj 2014.

5	Obezbijediti obuke za zaposlene koji rade na polju sajber bezbjednosti u okviru Nacinalnog CIRT-a i loklanih CIRT timova	Kako bi na što bolji i efikasniji način odgovorili na incidentne situacije, neophodno je obezbijediti obuke za stručno usavršavanje kadrova koje rade na rješavanju incidenata.	MIDT	Januar – decembar 2014.
6	Unaprijediti saradnju između javnog i privatnog sektora	Preko Nacionalnog Savjeta za sajber bezbjednost, obezbijediti procedure za razmjenu informacija između državnih organa i ključnih institucija iz privatnog sektora, naročito: • Internet provajderima • Agentom za .me domen • Bankarskim sektorom • Elektroprivredom • Kompanijama koje hostuju e-servise servise u Crnoj Gori U zavisnosti od sprovedene Analize, Savjet će definisati i način saradnje sa drugim subjektima.	MIDT MO MUP ANB	Jul 2014.
7	Izvršiti analizu prijetnji u sajber prostoru Crne Gore	Zbog konstantnog rasta broja usluga koje državni i privatni sektor pružaju putem interneta, kako građanima tako i drugim pravnim subjektima, moramo težiti ka zaštiti sajber prostora Crne Gore. Prvi korak jeste analiza sajber prijetnji.	MIDT MO MUP ANB	Decembar 2014.
8	Organizovati projekte i kampanje za promovisanje sigurnog korišćenja Interneta sa posebnim fokusom na zaštitu djece na internetu	Obezbijediti sigurnije internet okruženje za stanovnike Crne Gore i osposobljavanje korisnika kroz jačanje svijesti o sigurnom korišćenju Interneta. Posebnu pažnju posvetiti kampanjama i promociji zaštite djece na Internetu.	MIDT	Mart 2014.
	Jačanje specijalizovane jedinice za borbu protiv računarskog	Kako bi se omogućilo nesmetano procesuiranje djela protiv kompjuterskih podataka i sistema, djela koja se vrše pomoću kompjutera, potrebno je unaprijediti kapacitete specijalizovane		Do kraja

9	kriminala u okviru Uprave policije.	jedinice za borbu protiv računarskog kriminala u okviru Uprave policije.	MUP	2014.
10	Unaprijediti kapacitete za digitalnu forenziku	Potrebno je unaprijediti kapacitete Forenzičkog centra u Danilovgradu kako bi se omogućilo adekvatno prikupljanje i analiza elektronskog dokaznog materijala.	MUP	Septembar 2015.
11	Jačanje kapaciteta Ministarstva odbrane i Vojske Crne Gore u oblasti sajber odbrane	Definisati ulogu Ministartva odbrane i Vojske Crne Gore u sajber prostoru Crne Gore	Ministarstvo odbrane, Vojska Crne Gore	Mart 2015.
12	Organizovati konferencije/obuke na temu sajber bezbjednosti	Postaviti temelje za organizovanje regionalne konferencije/obuke na temu sajber bezbjednosti na godišnjem nivou. Na ovaj način se poboljšava regionalna saradnja, podiže nivo svijesti, i Crna Gora se promoviše kao jedna od vodećih zemalja u regionu na ovom polju.	MIDT MO MUP	Oktobar 2015.