IZVJEŠTAJ O

USPOSTAVLJANJU TIMOVA ZA UPRAVLJANJE INCIDENTNIM SITUACIJAMA NA INTERNETU U CRNOJ GORI – LOKALNI CIRT TIMOVI

SADRŽAJ:

UVOD.....5

ANALIZA TRENUTNE SITUACIJE.....6

PREGLED DALJIH AKTIVNOSTI.....11

ZAKLJUČAK.....12

PREDLOG ZAKLJUČAKA.....14

UVOD

Shodno Zakonu o informacionoj bezbjednosti, CIRT (Computer Incident Response Team/Tim za odaziv na incidentne situacije kod računarskih sistema) predstavlja organizacionu jedinicu Ministarstva za informaciono društvo i telekomunikacije (MIDT) i koordinira lokalnim CIRT timovima.

Obaveza formiranja lokalnih CIRT timova u institucijama jeste u cilju uspostavljanja Nacionalne CIRT (CIRT-ME) infrastrukture, koja je i predviđena **Strategijom sajber bezbijednosti Crne Gore 2013-2017** i pratećim akcionim planom.

Ministarstvo za informaciono društvo i telekomunikacije je shodno **Zaključku Vlade CG**, broj 06-1293/3 od 21.06.2012. godine, zaduženo da podnosi izvještaje o realizaciji zaključaka, kao i da nastavi aktivnosti na koordinaciji i implementaciji projekta uspostavljanja CIRT infrastrukture.

U cilju realizacije predmetnog Zaključka Vlade Crne Gore, zadužuju se državni organi, organi državne uprave, organi jedinica lokalne samouprave, pravna lica sa javnim ovlašćenjima i druga pravna i fizička lica koja ostvaruju pristup ili postupaju s podacima da, u saradnji sa **Nacionalnim CIRT-om**, formiraju svoje **lokalne CIRT timove** koji će se baviti uspostavljanjem sistema zaštite od računarskih bezbjednosnih incidenata na internetu i koji će imati direktnu komunikaciju sa Nacionalnim CIRT timom.

U daljem tekstu je predstavljena analiza trenutne situacije i stepen realizovanih aktivnosti kao i predlog aktivnosti za predstojeći period, a sa ciljem obezbjeđivanja informacione bezbjednosti i efikasne borbe protiv sajber kriminala u saradnji sa lokalnim CIRT timovima.

ANALIZA TRENUTNE SITUACIJE

Sistem informacione bezbjednosti može biti adekvatno implementiran tek kada je u okvirima jedne države uspostavljen sistem odgovornosti državnih organa, te kada postoji međusobna usklađenost i koordinacija aktivnosti.
Osnivanjem Nacionalnog CIRT-a pri Ministarstvu za informaciono društvo i telekomunikacije, napravljen je krupan korak ka sprječavanju i uklanjanju sajber prijetnji koje pogađaju državu i njene građane. CIRT se u saradnji sa ključnim institucijama u CG bavi detekcijom, praćenjem i suzbijanjem sajber napada i sajber kriminalom na nivou države. Nacionalni 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.

Na nacionalnom nivou, CIRT-ME je nastavio sa unapređenjem mehanizama proaktivnog i reaktivnog pristupa sajber sigurnosnim incidentima i prijetnjama. Kako bi na što bolji i efikasniji način odgovorili na incidentne situacije, neophodno je bilo obezbijediti kvalitetniju saradnju i nesmetanu razmjenu informacija između ključnih institucija na polju sajber bezbjednosti. Takođe, imajući u vidu da sajber napadi ne znaju za granice i da veliki broj sajber napada dolazi iz drugih zemalja, neophodno je bilo i uspostaviti i održavati saradnju sa relevantnim međunarodnim institucijama kao što su:

- **FIRST** (Forum of Incident Response Security Teams),
- **ITU** (International Telecommunication Union),
- **IMPACT** (International Multirateral Partnership Against Cyber Threats)
- **Trusted Introducer-**a - TERENA (Trans European Research and Education Networking Association),
- **Projekat Evropske unije - ACDC** (Advanced Cyber Defence Centre),
- **ENISA** (European Network and Information Security Agency),
- **NATO** (North Atlantic Treaty Organization)
- Potpisan je Memorandum o saradnji sa japanskim **JPCERT** timom,
- Direktna komunikacija sa velikim brojem CERT/CIRT timova na svjetskom nivou.

MIDT je, shodno zaključku Vlade, u proteklom periodu sproveo **planirane aktivnosti u okviru organizacije lokalnih CIRT timova u Crnoj Gori**. Kreirano je 15 lokalnih timova (*Tabela 1.)* koji

sarađuju sa članovima CIRT tima vezano za pitanja zaštite od računarskih bezbjednosnih incidenata na internetu.

R.br.	**Institucija**
1.	Ministarstvo odbrane
2.	Uprava policije
3.	Agencija za nacionalnu bezbjednost
4.	Državna revizorska institucija
5.	Ministarstvo saobraćaja i pomorstva
6.	Monstat
7.	Opština Kotor
8.	Opština Berane
9.	Uprava za zaštitu konkurencije
10.	Vrhovno državno tužilaštvo
11.	Ministarstvo pravde
12.	Opstina Pljevlja
13.	Opština Cetinje
14.	Direkcija za zaštitu tajnih podataka
15.	Vojska CG

Tabela 1. Prikaz institucija koje su formirale lokalne CIRT timove ili definisale kontakt osobu

Kroz međusobnu saradnju i redovne kontakte omogućena je razmjena informacija između formiranih lokalnih timova, efikasna komunikacija u istragama i rješavanju računarsko-bezbjednosnih incidenata čime se podstiče razvoj smjernica za olakšavanje razmjene podataka kako na nacionalnom tako i na međunarodnom nivou, uključujući garancije zaštite podataka, procedura, tehničkog i pravnog aspekta.

Tokom 2012./2013 godine **organizovane su obuke za članove lokalnih CIRT timova** kako u zemlji tako i u inostranstvu. Članovi lokalnih CIRT timova imali su priliku da se obučavaju na raznim edukativnim skupovima, konferencijama, kursevima, kao što su:

- U okviru **IPA twinning projekta**, „Strenghtening administrative capacities in information society“, održana je obuka pod nazivom “Elementi ICT bezbjednosti”.
- U **Ankari** je organizovana i uspješno završena 15-dnevna obuka na temu sajber bezbjednost pod pokroviteljstvom NATO-a.
- U **Ohridu** je takođe pod pokroviteljstvom NATO-a organizovana 6-dnevna obuka čiji je cilj bio razumijevanje važnosti izgradnje efektivne sajber odbrane kao i internacionalnih pravnih izazova kod efektivne sajber odbrane.
- U **Bugarskoj** je CG uzela učešće u prvoj prekograničnoj sajber vježbi dizajniranoj kako bi testirali sposobnosti odgovora na računarske incidente evropskih zemalja i poboljšali spremnost u slučaju eventualnog sajber napada.
- U organizaciji **IMPACT** stručnjaci iz **Malezije** su organizovali 12-dnevnu stručnu obuku u Podgorici za predstavnike državnih organa.
- Predstavnici **CIRT-a** su boravili u centrali **IMPACT-a** u **Maleziji** u trajanju od 7 dana.
- Predstavnik **CIRT-a** je učestvovao u definisanju pravilnika o izradi Strategije o sajber bezbjednosti u organizaciji **NATO-a u Ženevi**.
- Završena obuka za 3 predstavnika **CIRT-a** Crne Gore, koja je održana u **Japanu (CERT)**, u trajanju od 4 mjeseca.

U sklopu svojih svakodnevnih aktivnosti CIRT je nastavio sa uspješnim radom na rješavanju incidentnih situacija koje se mogu prijaviti preko portala CIRT-a, www.cirt.me. Portal je uspostavljen 2012. godine. Trenutno je objavljeno preko **60 informacija** o sajber bezbijednosti (članci, obavještenja, sigurnosna upozorenja, brošure, savjeti za zaštitu i drugo).
Neki od prijavljenih incidenata su zahtijevali i prekograničnu saradnju i razmjenu informacija sa ostalim Nacionalnim CERT timovima sa kojima smo uspostavili saradnju, kao što su:

- CERT Hrvatske (CARNET)
- Slovenački CERT (SICERT)
- CERT Holandije (AAB GCIRT)
- CERT Francuske (Cert-IST)
- Njemački CERT (S-CERT)

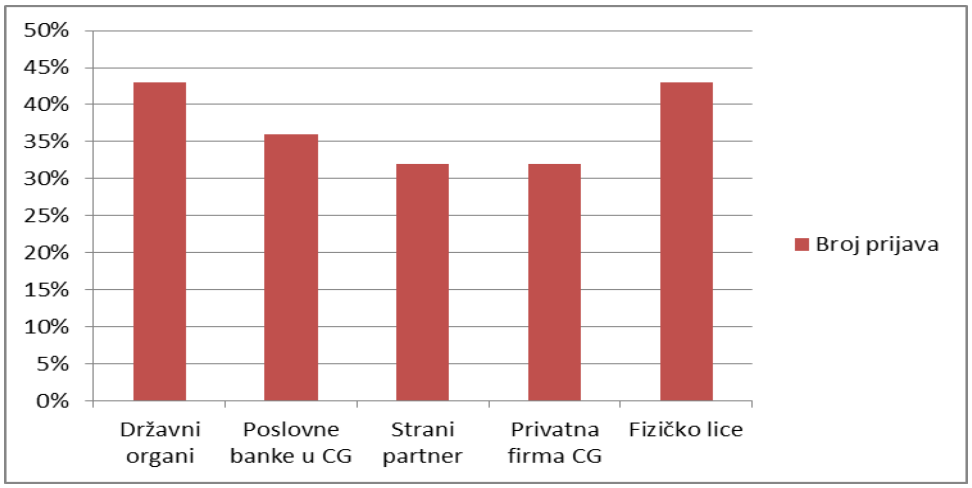
- Italijanski CERT (CERT Italy)
- Bugarski CERT (CERT Bulgaria)
- CERT Indije (CERT-In)
- USA CERT (US-CERT)

U tabeli (*Tabela2*) je predstavljen broj prijavljenih incidenata za 2013. godinu.

R.br.	Institucija	Broj prijava	Vrsta incidenta
1.	Državni organi	13	Web defacement, DOS i DDoS napad,
2.	Poslovne banke u CG	3	Phishing
3.	Inostrane banke	3	Phishing
4.	Strani partner	2	MiniDuke- trojanac (sajber špijunaža)
5.	Privatna firma CG	2	Brute force
6.	Fizičko lice	13	Zloupotreba profila na facebook-u, twitter-u, skype-u

Tabela 2. Spisak prijavljenih incidenata

Slijedi i grafički prikaz incidentnih situacija:



Grafički prikaz prijavljenih incidenata za 2013. godinu

Na osnovu zaključka Vlade, neophodno je u **narednom periodu uspostaviti lokalne CIRT timove** (kontakt osobe) u svim drugim državnim organima i obezbijediti njihovo uvezivanje sa nacionalnim CIRT-om. Spisak državnih organa u koje je potrebno formirati lokalne CIRT timove u ovom trenutku, predstavljen je u *Tabeli 3*.

R.br.	**Institucija**
1.	Ministarstvo vanjskih poslova i EI
2.	Ministarstvo održivog razvoja i turizma
3.	Ministarstvo prosvjete i sporta
4.	Poreska uprava
5.	Uprava carina
6.	Skupština CG
7.	Sudovi, sudski savjet
8.	JP Aerodromi
9.	Univerziteti u CG
10.	Fond PIO
11.	Fond za zdravstveno osiguranje
12.	Zavod za zapošljavanje
13.	Ostale opštine

Tabela 3. Spisak institucija u kojima je neophodno formiranje lokalnog CIRT tima ili definisanje kontakt osobe

PREGLED DALJIH AKTIVNOSTI

Nacionalni CIRT tim će u narednom periodu raditi i na sljedećim aktivnostima:

- **podsticanje i pomoć prilikom uspostavljanja ostalih CIRT-ova** u nacionalnoj CIRT infrastrukturi, kroz saradnju sa upravom, savjetovanje i edukaciju zaposlenih – članova CIRT-ova;
- **definisanje osnovnih potrebnih funkcionalnosti CIRT-ova**, njihove međusobne komunikacije, kao i odnosa prema Nacionalnom CIRT-u (izvještavanje, razmjena informacija između CIRT-ova i sa drugim relevantnim tijelima van Crne Gore);
- **koordinacija zajedničke saradnje** sa ostalim relevantnim organima javne uprave, privatnog sektora i međunarodnih institucija.

Nacionalni CIRT će u narednom periodu, definisati način saradnje sa predstavnicima **privatnog sektora** koji upravljaju sa kritičnom informatičkom infrastrukturom, kao što je:

- bankarski sektor,
- elektroprivreda,
- telekomunikacioni sektor,
- internet provajderi i dr.

Osnova dalje saradnje sa privatnim sektorom podrazumjeva sljedeće aktivnosti:

- Razvoj procesa međusobne komunikacije i njegovih elemenata;
- Razmjenu informacija i iskustava;
- Organizaciju zajedničkih događaja: sastanaka, konferencija, okruglih stolova, foruma, seminara, panela;
- Stručno usavršavanje kroz organizaciju seminara, obuka, konferencija, te podsticanje uključivanja stručnjaka obje strane;
- Osnivanje zajedničkih radnih grupa za razna područja od obostranog interesa;

Tako uspostavljena hijerarhija treba da omogući nesmetanu razmjenu informacija o računarskim bezbjednosnim problemima, blagovremena upozorenja o računarsko-bezbjednosnim rizicima i efikasnu komunikaciju u istragama i rješavanju računarsko-bezbjednosnih incidenata, kako u Crnoj Gori, tako i sa odgovarajućim inostranim organima.

ZAKLJUČAK

U okviru državne uprave, a shodno zaključku Vlade, neophodno je da postoji definisana organizaciona hijerarhija koja će najefikasnije i dugoročno održivo obezbijediti sigurno i adekvatno upravljanje informacionom bezbjednošću u Crnoj Gori.

Zbog konstantnog rasta broja usluga koje državni organi i privatni sektor pružaju, kako građanima tako i drugim pravnim subjektima, potrebno je na nivou lokalnih CIRT timova razviti procedure zaštite.

Potrebno je da svi **lokalni CIRT timovi svih ključnih institucija adekvatno rukuju ICT infrastrukturom** u cilju zaštite povjerljivosti, cjelovitosti i dostupnosti sistema. Moramo biti spremni za sajber incidente (napade), kako bi eventualna šteta od istih bila manja. Nije dovoljno samo formiranje timova , već se problem bezbjednosti mora pratiti u kontinuitetu.

Nacionalni CIRT tim će u narednom periodu raditi i na sljedećim aktivnostima:

- **Uspostaviti CIRT timove u ostalim državnim organima** i povezati ih sa nacionalnim CIRT-om a;
- **Definisati osnovne funkcionalnosti CIRT-ova**, njihove međusobne komunikacije, kao i odnosa prema Nacionalnom CIRT-u (izvještavanje, razmjena informacija između CIRT-ova i sa drugim relevantnim tijelima van Crne Gore);
- **Poboljšati saradnju** između ključnih institucija i **potpisati protokole o saradnji** na polju sajber bezbijednosti. U tim protokolima treba jasno definisati načine saradnje u cilju podsticanja daljeg razvoja boljih odnosa i jačanja stalnih napora na područjima od zajedničkog interesa u procesu implementacije i realizacije koordinisanih aktivnosti u oblasti sajber bezbjednosti;
- **Koordinacija zajedničke saradnje** sa ostalim relevantnim organima **javne uprave i međunarodnih institucija**;
- Uspostaviti **saradnju sa predstavnicima ključnih institucija iz privatnog sektora** (banke, internet provajderi, elektroprivreda, mobilni operatori, domen i drugi);
- Uspostavljanje **real-time mehanizama za koordinaciju sa drugim državama** u cilju pravovremenog reagovanja na sajber incidente;

- Sprovođenje **adekvatnih obuka** kako bi se unaprijedile vještine i stručnost službenika u lokalnim CIRT timovima;
- Stvaranje **svijesti i promovisanje preventivnih mjera** na svim nivoima;

Crna Gora kao odgovoran subjekt međunarodnih odnosa mora **uspostaviti osnovne pretpostavke za razvoj sigurnog sajber prostora od nacionalnog interesa** Što će dati nesumnjiv doprinos daljem jačanju nacionalne i globalne sigurnosti, i što će imati i neposredan uticaj na smanjenje stope organizovanog sajber kriminala koji predstavlja rastuću prijetnju svjetskom miru.

U tom pogledu, od velikog značaja za državu je **uspostavljanje i formiranje lokalnih timova za upravljanje incidentnim situacijama u sajber prostoru** u državnim organima, organima državne uprave, organima lokalne samouprave, pravnim licima, kao i pravovremena razmjena svih informacija koje se odnose na sajber zaštitu.