Vlada Crne Gore

Ministarstvo za informaciono društvo i telekomunikacije

ANALIZA
prijetnji u sajber prostoru Crne Gore

Decembar, 2014.

Uvod

Vlada Crne Gore je usvojila Strategiju Sajber bezbjednosti u Crnoj Gori od 2013-2017. godine. Implementacija Strategije treba da doprinese podizanju stepena sajber bezbjednosti. U cilju realizacije, usvojen je Akcioni plan kojim je, kao jedna od aktivnosti koju je neophodno sprovesti, predviđena Analiza prijetnji u sajber prostoru u Crnoj Gori.

Današnje informaciono društvo nezamislivo je bez razvoja sistema informacione bezbjednosti. Informaciona bezbjednost u svim segmentima jedne države predstavlja važnu pretpostavku za stvaranje kvalitetnog informacionog društva.

Činjenica da moderno društvo danas u potpunosti zavisi od tehnologije dokazuje da su informacioni sistemi neophodni za funkcionisanje istog. Organizacije su suočene sa raznim vrstama prijetnji po sigurnost informacija. Što je organizacija zavisnija od informacionog sistema, više je osjetljiva i ranjiva na različite napade. Prema mnogim nezavisnim izvorima sofisticiranost i složenost prirode sajber napada će kontinuirano nastaviti da raste.

Jedna od glavnih tema interesovanja državnih struktura je zaštita podataka tj. informacionih sistema. U zavisnosti od toga da li je informacioni sistem od vitalnog značaja, ključne institucije iz državnog, kao i iz privatnog sektora trebaju da štite informacije zbog integriteta, dostupnosti i povjerljivosti podataka. Za banke je od presudnog značaja integritet informacija zbog finansijskog poslovanja. Za provajdere Internet usluga najvažnije su raspoloživost i pouzdanost informacija zbog kontinuiteta pružanja usluga, dok je za privrednike najvažnija povjerljivost informacija zbog opstanka na tržištu i uspješnog poslovanja.

Svjesna značaja razvoja i primjene informacione bezbjednosti, Crna Gora je u prethodnom periodu napravila značajne korake u tom pravcu.

U Crnoj Gori formiranjem CIRT-a, kao organizacione jedinice u Ministarstvu za informaciono društvo i telekomunikacije, postavljene su osnove za obavljanje poslova koji se odnose na prevenciju, obradu i otklanjanje posledica od računarskih bezbjednosnih incidenata na internetu i drugih rizika bezbjednosti informacionih sistema u cilju stvaranja održivog informacionog društva.
Jedan od ciljeva je i da se omogući rano otkrivanje informacionih prijetnji i incidenata na nacionalnom nivou i da se adekvatno reaguje i odgovori na iste.

Zbog konstantnog rasta broja usluga koje državni i privatni sektor pružaju putem interneta, kako građanima, tako i pravnim subjektima, moramo težiti ka zaštiti sajber prostora Crne Gore. Prvi korak jeste analiza sajber prijetnji.

Cilj ove analize je da identifikuje potencijalne izvore prijetnji u sajber prostoru koje mogu uticati na informacione sisteme. Za analizu je neophodno sagledati dosadašnje prijetnje na nacionalnom nivou sa osvrtom na regionalni i globalni nivo. Izvori prijetnje se

definišu zavisno od situacije, a to su uglavnom prirodni faktori, ljudski faktori i faktori okruženja (tehničke greške i nepravilnosti, ranjivost sistema i slično).
U izradi analize korišćeni su podaci kojim raspolažu Ministarstvo za informaciono društvo i telekomunikacije, Zavod za statistiku Crne Gore, kao i organizacije Kaspersky, ENISA, Verizon izvještaj o kompromitovanim podacima i dr.

Koristeći se unaprijed iznesenom metodologijom, a kako bi stvorili što bolju sliku o crnogorskom sajber prostoru, veoma je bitno sagledati statističke podatke upotrebe informaciono-komunikacionih tehnologija u Crnoj Gori.

Takođe, u Analizi su prikazani statistički podaci o broju i vrsti najčešćih prijetnji u sajber prostoru, sa trendom rasta, na nacionalnom nivou (kompjuterski kriminal, virusi, napadi, zloupotreba profila i drugi).

Poseban fokus bi trebalo posvetiti upravljanju nacionalnim sajber prijetnjama i dati smjernice u koordinaciji sa lokalnim akterima i internacionalnim partnerima u cilju zaštite informacionih sistema.

Sajber prijetnje na globalnom nivou

Polje djelovanja sajber kriminalaca prevazilazi granice pojedinačnih zemalja i za njihovo adekvatno suzbijanje potrebna je međunarodna saradnja. Svakog dana pojavljuju se na hiljade novih virusa i stotine novih vrsta napada. Nekada je akcenat bio na kreiranju mreža zaraženih računara, ali sada kriminalci biraju cloud servise i mobilne uređaje. Napadači i prijetnje se dosta mijenjaju, ali su izvdojeni trenutno najaktuelniji.

Sajber napadači

- **Korporacije:** Glavni cilj korporacija je da steknu kompetetivnu prednost u odnosu na konkurenciju. Obično se radi o sakupljanju informacija vezanih za biznis, preuzimanje zaštićenih intelektualnih dostignuća, otkrivanje tuđih ponuda prilikom tendera i sl. Korporacije ili unajmljuju plaćenike za ove poslove ili ako su dovoljno velike imaju svoje odsjeke za sajber špijunažu.

- **Države:** Jasno je da su dimenzije ovih napada u konstantnom širenju. Više država je razvilo sposobnosti koje mogu biti korišćene za različite vrste napada, bilo protiv drugih vlada ili privatnih institucija. Napadi su najviše usmjereni ka otkrivanju državnih i vojnih tajni, obavještajnih podataka, kao i prema kritičnoj infrastrukturi. Metode napada izrazito variraju i imaju veoma visok procenat uspješnosti.

- **Haktivisti**: Haktivisti predstavljaju grupu napadača koji uživaju veliki publicitet, npr. Anonimusi. Oni su ideološki motivisani pojedinci, koji dinamički formiraju grupe, obično bez centralne organizacione strukture. Njihova glavna motivacija je odbrana ideja. Biraju mete koje će stvoriti što veći odraz u medijima, pa zato biraju sajtove vlada, velikih kompanija i slično.

- **Sajber teroristi:** Ovakve grupe obično ciljaju nacionalnu bezbjednost i cjelokupno društvo. Karakterišu se primjenjivanjem represivnih mjera, kako bi uticali na proces donošenja odluka, a sve u cilju postizanja svojih ciljeva. Uobičajeno je da napadaju kontrolu saobraćaja, vojnu infrastrukturu, vladine sisteme i sl.

- **Sajber kriminalci:** Ove grupe su najpoznatije od svih sajber napadača. Njihova glavna motivacija je sticanje profita nelegalnim sajber aktivnostima. Umiješani su u sve vrste prevara sa elektronskim finansijama, trgovinom, platnim rješenjima, otkupom, sajber kriminalnim uslugama, isporučivanje i izrada malicioznog koda.

Ove grupe imaju velike mogućnosti u sprovođenju zadataka, mogu biti globalno povezane i mogu lako ostvariti pristup neophodnim resursima za sprovođenje napada. Bitno je razlikovati korisnike i provajdere malvera. Oni koji razvijaju takve programe, smatraju se najvještijim napadačima, zato što drugi koriste njihove alate kako bi sprovodili napade.

- **Sajber borci:** Grupa građana koji su motivisani na nacionalnoj osnovi. Oni iz patriotskih razloga pokreću koordinisane sajber napade. Obično se smatraju podvrstom haktivista.

- **Skript prepisivači (script kiddies** u originalu)**:** su pojedinci koji tek ulaze u svijet sajber napada. Oni ne poznaju dovoljno tehnike i alate, već samo kopiraju napad iskusnijih hakera. Zbog ovoga oni obično nisu upoznati sa posledicama koje mogu da proizvedu.

Sajber prijetnje

Kako bi na najbolji način razumjeli sajber prijetnje na nacionalnom nivou, prvo moramo sagledati trenutno stanje na globalnom nivou. U nastavku su prikazani izvještaji o sajber prijetnjama koje na godišnjem nivou objavljuju ugledne organizacije KASPERSKY i ENISA, kao i izvještaj američke kompanije Verizon.

KASPERSKY – izvještaj o globalnim sajber prijetnjama

Za izradu ovog izvještaja, Kaspersky je sproveo anketu, Bezbjednosne prijetnje i kompromitovanje podataka na internetu (IT security threats and data breaches), sa 3,900 korespondenata iz 27 zemalja svijeta. Izvještaj se odnosi na prijetnje za poslovni sektor tj. mala, srednja i velika preduzeća tokom 2013.godine. Prema rezultatima ankete, došlo se do sljedećih ključnih saznanja:

- Spam je eksterna prijetnja br.1., 64% anketiranih lica je izjavilo da ima problema sa spamom.
- Virusi, trojanci i ostale vrste malvera predstavljaju problem za 61% korespondenata.
- 94% kompanija se susrelo sa sajber bezbjednosnim incidentima čiji je izvor izvan prostorija kompanije.
- 12% kompanija su bile meta ciljanih napada.
- Glavna interna prijetnja su ranjivosti u postojećim softverskim rješenjima koje koriste (36%), kao i zaposleni koji nisu upoznati sa bezbjednosnom politikom i pravilima, što dovodi do nenamjernog curenja podataka (29%)

U nastavku slijede detaljne tabele eksternih i internih prijetnji:

Eksterne prijetnje									
	Globalno	Rusija	Kina	S.Amerika	Z.Evropa	Istok	Pacifik	Bliski istok	Japan
Spam	64%	75%	63%	72%	63%	63%	65%	62%	38%
Virusi, trojanci, spyware i drugi maliciozni programi	61%	78%	59%	66%	54%	62%	68%	51%	45%
Phishing napadi	38%	25%	41%	57%	41%	33%	39%	24%	23%
Upadi u mrežu / hakovanje	25%	21%	40%	21%	22%	23%	35%	24%	21%
Krađa mobilnih uređaja	22%	15%	25%	19%	25%	23%	25%	8%	15%
DoS, DDoS	18%	17%	34%	15%	17%	17%	20%	22%	13%
Krađa većeg hardvera	16%	11%	20%	12%	16%	18%	22%	9%	7%
Industrijska špijunaža	16%	24%	26%	6%	12%	16%	21%	10%	9%
Ciljani napadi	12%	9%	20%	10%	10%	12%	18%	13%	6%
Kriminalna šteta (uključujući požar)	6%	5%	6%	5%	5%	8%	10%	3%	3%
Nema problema	6%	3%	1%	7%	7%	6%	4%	11%	20%

Tabela 1: eksterne prijetnje

Interne prijetnje									
	Globalno	Rusija	Kina	S.Amerika	Z.Evropa	Istok	Pacifik	Bliski istok	Japan
Ranjivosti u postojećem softveru	36%	50%	38%	33%	32%	37%	37%	23%	26%
Nenamjerno širenje/curenje podataka od strane zaposlenih	29%	34%	42%	26%	26%	25%	34%	25%	23%
Gubitak/krađa mobilnih uređaja od strane zaposlenih	26%	19%	27%	22%	29%	24%	29%	25%	28%
Namjerno širenje/curenje podataka od strane zaposlenih	21%	22%	32%	12%	18%	21%	30%	18%	14%
Širenje/curenje podataka putem mobilnih uređaja	20%	18%	30%	16%	18%	22%	27%	13%	11%
Bezbjednosni propust trećeg lica/kompanije	16%	10%	25%	14%	15%	17%	23%	11%	10%
Prevare od strane zaposlenih	16%	10%	25%	14%	15%	17%	23%	11%	10%
Nema problema	17%	14%	9%	26%	19%	14%	11%	30%	20%

Tabela 2: Interne prijetnje

Kada su u pitanju korisnici PC i mobilnih uređaja, statistika Kaspersk-og za 2013. godinu je sledeća:

- U 2013. godini, Kasperky je neutralisao 5,188.740.554 sajber napada na korisničke računare i mobilne uređaje;
- Otkriveno je 104,427 novih modifikacija malicioznih programa za mobilne uređaje;
- Kaspersky je neutralisao 1,700.870.654 napada koji su lansirani sa online resursa lociranih u svim krajevima svijeta;
- Detektovano je skoro 3 milijarde napada malverom na korisničke računare;
- 45% online napada koje je neutralisao Kaspersky dolaze iz malicioznih online resursa koji su locirani u SAD i Rusiji.

ENISA – pregled sajber prijetnji u 2013. godini

Za izradu ovog dokumenta, ENISA je koristila izvještaje nacionalnih i internacionalnih organizacija kao što su CERT/CIRT timovi, državne institucije, akademija, industrija, štampa, kao i individualne eksperte za sajber bezbjednost.

Na osnovu prikupljenih informacija, došlo se do sljedećih ključnih zaključaka:

- Sofisticiranost napada i korišćenih alata je u stalnom porastu;
- Jasno je da sve više država razvija svoje sposobnosti da infiltriraju razne vrste meta iz državnog i privatnog sektora kako bi ostvarile svoje ciljeve;
- Sajber prijetnje su prenešene i na mobilne uređaje;
- Pojavila su se dva nova digitalna borilišta: veliki podaci (eng. *big data*) i Internet stvari (eng. *Internet of things*);
- Policija ima sve više uspjeha u borbi protiv sajber kriminala. Uhapšene su kriminalne grupe koje stoje iza nekih od većih sajber napada (*Police virus, Silk road, Blackhole);*
- Vendori su ubrzali svoje odgovore na prijetnje i ranjivosti češćim ažuriranjem svojih proizvodaOvdje ćemo govoriti o najzastupljenijim prijetnjama tokom 2013. godine po ENISA-inom izvještaju (ENISA Threat Landscape 2013.)

- Zlonamjerni kod (Drive-By download)

Prirodno je da je ovaj vid prijetnje na prvom mjestu, jer je glavni vid interakcije korisnika sa Internetom preko web pretraživača. Zbog ovoga su web serveri i web usluge postale najbitnija osnova za napade. Hakeri se trude da zaraze ove servise sa zlonamjernim kodom, kako bi se onda pretraživači korisnika inficirali.

Prema broju, ovi napadi drže prvo mjesto. Primjetan je prelaz sa botnet-ova koji su nekada korišteni za širenje zlonamjernog koda na web sajtove. Java propusti su i dalje najviše korišćeni, a mobilne platforme su podjednako zastupljene sa posebnim exploit alatima.

- Maliciozni programi (crvi i trojanci)

Tokom posmatranog perioda, izdvojeno je na hiljade varijanti različitih malvera. Do ovoga je došlo zbog široke dostupnosti alata koji generišu custom malvare. Samo mala izmjena u kodu zlonamjernih programa je dovoljna da kreira potpuno drugačiji potpis, te ti kodovi ne mogu biti detektovani konvencionalnim anti-malvare alatima.
Primjetan je rast mobilnog malvare i posebnih trojanaca. Zbog primjena principa polimorfnog koda u alatima za generisanje zlonamjernog koda i običan korisnik koji nije stručnjak može kreirati novi oblik zlonamjernog koda.

- Code Injection

Grupa alata kojima se vrše ovi napadi je ostala nepromijenjena i koriste principe: Cross-Site-Scripting (XSS), Directory Traversal, SQLi i Cross-Site Request Forgery (CSRF).
Tokom 2013. bio je primjetan porast broja napada na poznate CMS-ove (Wordpress, Joomla, Drupal). Zbog njihove široke primjene i miliona sajtova koji ih koriste oni su postali značajne mete.
Drugi zanimljiv trend je pokretanje ogromnih automatizovanih napada iz cloud servisa.

- Exploit Kit-ovi

Ovo su glavni alati svih hakera, predstavljaju svojevrsne sajber švajcarske noževe. Oni su upakovani sa hiljadama poznatih propusta i redovno se update-uju. Upravo zbog ovog modela gdje developeri ovih alata nude podršku za svoje proizvode počinju da se javljaju novi oblici sajber usluga. Kako su redovno update-ovani onda imaju i najnovije propuste, pa su zbog toga i uspješniji u napadima.

- Botnetovi

Mreža kompromitovanih računara, koji su kontrolisani na daljinu i dalje predstavlja ozbiljnu prijetnju. Ovo je jedan od oblika zlonamjerne infrstrukture koji postoji najduže i redovno se organizuju kampanje za njihovo gašenje (botnet takedown). Kako bi prikrili svoje botnetove developeri su se dosjetili da koriste P2P tehnologiju za komuniciranje sa C&C serverima.
Ostali napadi kao DoS, krađe identiteta, spam i slično nisu se značajnije izmijenili.

U nastavku je prikazana tabela najvećih prijetnji u 2013. godini sa trendom rasta u odnosu na prethodnu godinu, kao i tabela učešća identifikovanih grupa napadača u najvećim prijetnjama.

	Glavne prijetnje – 2012	Trend rasta	Glavne prijetnje – 2013	Trend rasta	Promjena pozicije
1	Drive-by download napadi (web bazirani napadi)	⇧	Drive-by download napadi (web bazirani napadi)	⇧	⇨
2	Virusi/trojanci/crvi	⇧	Virusi/trojanci/crvi	⇧	⇨
3	Code injection (umetanje koda)	⇧	Code injection (umetanje koda)	⇧	⇨
4	Exploit kits	⇧	Exploit kits	⇧	⇨
5	Botnetovi	⇧	Botnetovi	⇨	⇨
6	DoS, DdoS	⇨	Fizička krađa/gubitak/šteta	⇧	⇧
7	Phishing	⇨	Krađa identiteta/Prevara	⇧	⇧
8	Kompromitovanje povjerljivih podataka (*Data Breach*)	⇧	DoS, DdoS	⇧	⇩
9	Rogueware/Ransomware/ Scareware	⇨	Phishing	⇧	⇩
10	Spam	⇩	Spam	⇨	⇨
11	Ciljani napadi	⇧	Rogueware/Ransomware/ Scareware	⇧	⇩
12	Fizička krađa/gubitak/šteta	⇧	Kompromitovanje povjerljivih podataka (*Data Breach*)	⇧	⇩
13	Krađa identiteta	⇧	Curenje podataka (Information leakage)	⇧	⇧
14	Curenje podataka (Information leakage)	⇧	Ciljani napadi	⇧	⇩
15	„Trovanje“ pretraživača (uklonjeno sa liste 2013)	⇨	*„Watering hole“* napad	⇧	⇧
16	Inficiranje certifikata (integrisan sa trojancem/crvom)	⇧			

Tabela 3: Najveće prijetnje i trend rasta

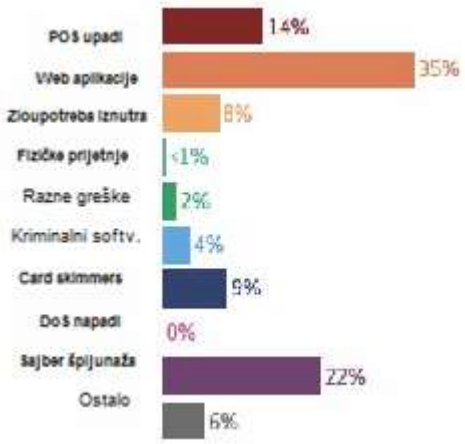
Mogući napadači									
	Korporacije	Države	Hakti visti	Sajber teroristi	Sajber kriminalci	*Sajber borci*	*Script kiddies*	Online društveni hakeri	Zaposleni
Drive-by download napadi (web bazirani napadi)		✓			✓				
Virusi/trojanci/crvi		✓		✓	✓	✓		✓	✓
Code injection (umetanje koda)	✓	✓	✓	✓	✓	✓	✓		
Exploit kits			✓	✓	✓	✓	✓		
Botnetovi	✓	✓	✓	✓	✓	✓			
Fizička krađa/gubitak/šteta	✓	✓	✓	✓	✓	✓	✓	✓	✓
Krađa identiteta/Prevara	✓	✓	✓	✓	✓	✓	✓	✓	✓
DoS, DdoS		✓	✓	✓	✓	✓	✓		✓
Phishing	✓	✓			✓			✓	
Spam	✓				✓			✓	
Rogueware/Ransomware/ Scareware					✓				
Kompromitovanje povjerljivih podataka (*Data Breach*)	✓	✓	✓	✓	✓	✓	✓		✓
Curenje podataka (Information leakage)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ciljani napadi	✓	✓	✓	✓	✓	✓		✓	
„Watering hole“ napad	✓	✓			✓	✓			

Tabela 4. Napadači

VERIZON – izvještaj o kompromitovanju povjerljivih podataka u 2013. godini

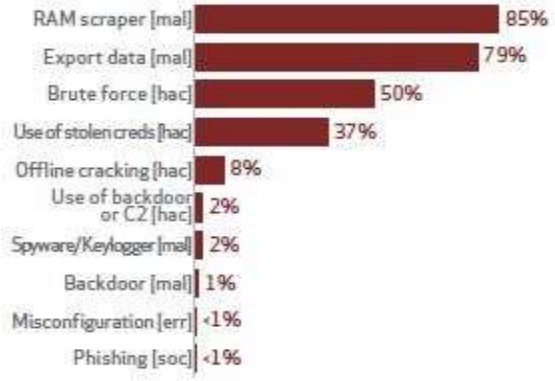
Ovaj izvještaj uključuje podatke forenzičkih istraživanja širom svijeta ne zaobilazeći Crnu Goru. Izvještaj je obradio prikupljene podatke za više od 60,000 incidenata i izašao sa ukupno devet klastera koje imaju zajedničke prijetnje (u smislu dejstva, ciljeva i učesnika). Tim je ustanovio da sledeće kategorije obuhvataju gotovo 90% svih incidenata prikazane na slici 1: POS upadi (1%), web aplikacije (6%), zloupotreba iznutra (18%), fizičke prijetnje (14%), maliciozni softveri (20%), card skimming (1%), razne greške (25%), DoS napadi (3%), i sajber špijunaža (1%). Izvještaj takođe sadrži i preporučene aktivnosti, od strane kompanije Verizon, koje će umanjiti rizik od potencijalnih prijetnji.
Sveobuhvatna procjena pokazuje da je 2013. godina tranzicije iz geopolitičkih napada u krupne napade na sisteme platnih kartica.

Slika 1. 10 najčešćih incidenata



Slika 2. Prikaz kompromitovanja podataka

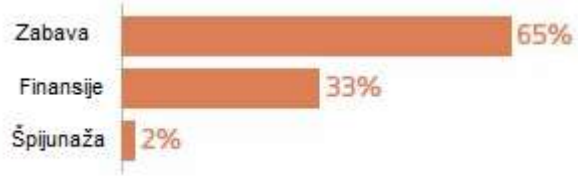
- **Upadi na platna mjesta (POS)** podrazumijevaju udaljene napade u prostoru gdje je aktuelan sistem platnih kartica. Zločini uključuju manipulaciju ili zamjenu uređaja (terminala). U izvještaju se navodi da je od 198 incidentnih slučajeva, u svim slučajevima potvrđeno je kompromitovanje podataka. Na slici ispod se nalaze najčešće prijetnje koje pogađaju ovu kategoriju. Na prvom mjestu je RAM scrapper, zlonamjerni softver koji snima podatke platnih kartica iz jednog sistema u RAM memoriju.



Slika 3. 10 najčešćih prijetnji unutar POS upada

Preporučene kontrole : ograničiti udaljeni pristup, forsirati pasvord polise, instalacija antivirusa, monitoring mreže i drugo.

- **Napadi na web aplikacije** su incidenti najčešće sporevedeni koristeći ranjivosti u web aplikaciji. Dodatan problem stvara činjenica da mnoge kompanije koje nude ovu vrstu servisa nemaju sistem autentifikacije. U izvještaju se navodi da od 3,937 ukupnih incidenata, u 490 slučajeva je potvrđeno kompromitovanje podataka. Mnogi napadi su bili ciljani napadi kako bi preuzeli kontrolu nad serverom za DDoS kampanje. Na slici možemo vidjeti da su motivi najčešće iz razonode i zabave dok je špijunaža na poslednjem mjestu.



Slika 4. Prikaz najčešćih motiva napada

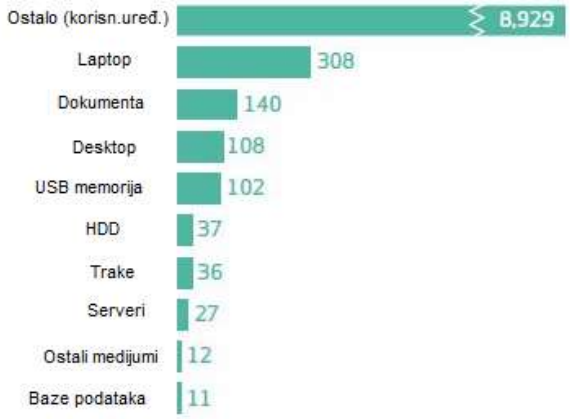
Preporučene kontrole: provjeriti i preispitati CMS, forsirati polise zaključavanja, monitoring spoljašnjih konekcija i drugo.

- **Zloupotreba iznutra**
  Incidenti koji obuhvataju nedozvoljeno ili zlonamjerno korišćenje organizacionih resursa. Uglavnom se misli na zloupotrebu iznutra, ali česta je zloupotreba i sa strane (dosluh) i partnera. Od ukupnih 11,698 incidenata, u 112 incidenata je potvrđeno kompromitovanje podataka. Većina zločina su počinjeni iz lične ili finansijske koristi.
  U 2013. godini zabilježeno je povećanje insajder špijunaže čije su mete bili interni podaci i otkrivanje poslovnih tajni. Na slici 5 možemo vidjeti najčešće prijetnje zloupotrebe iznutra.

Slika 5. Pregled prijetnji zloupotrebe iznutra

Preporučene kontrole: Pojačati kontrolu pristupa, kontrola korisničkih naloga, objavljivanje rezultata revizije i ostalo.

- **Krađa i gubitak**
  Incidenti u kojima informacije ili podaci nestaju bilo slučajno ili namjerno. Od ukupno 9.704 incidenta, u 116 incidenata je potvrđeno kompromitovanje.
  Gubitak se javlja češće nego krađa i to češće u kancelarijama nego iz automobila ili stana. I dok su lične i zdravstvene informacije najviše izložene, većina gubitaka je prijavljena zbog otkrivanja, a ne zbog prevare.



Slika 6. Deset najšešćih vrsta krađa

Preporučene kontrole: enkriptovati uređaje, ne ostavljati ih na javnim mjestima, raditi backup, zaključavati uređaje i slično.

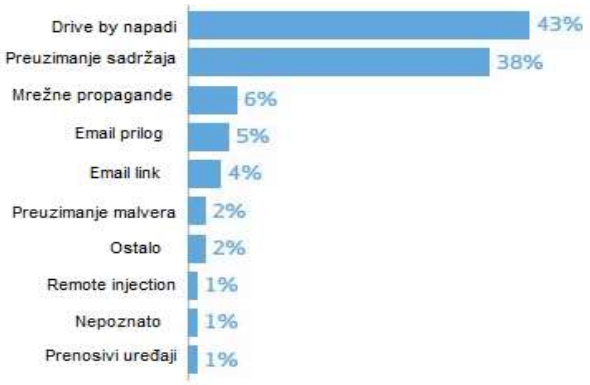
- **Razne greške**
  Incidenti u kojima nenamjerne radnje ugrožavaju bezbjednost informacione imovine. Nisu uključeni izgubljeni uređaji koji su grupisani u prethodnoj kategoriji (krađa/gubitak) Izvještajem se navodi da od ukupno 16,554 incidenata, u 412 incidenata je potvrđeno kompromitovanje podataka. Treba napomenuti da je najveći broj inidenata napravljen i uzrokovan od strane poslovnih partnera.

Slika 7. Prikaz 10 najčešćih greški

Preporučene kontrole: implementacija softvera za prevenciju gubitka podataka i slično.

- **Kriminalni softver**
  Ovdje spadaju razni tipovi malvera dizajnirani za različite svrhe i namjene. Od ukupno 12,535 incidenata u 50 incidenata je potvrđeno komrpomitovanje podataka. Primarni cilj je da se preduzme kontrola nad sistemima za nezakonite svrhe kao što su krađa podataka, DDoS napadi, spamovanje i slično.

Slika 8. Prikaz najčešćih softvera

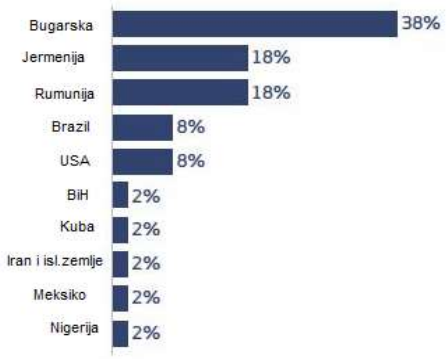


Slika 9. Prikaz najčešćih vektora za maliciozne akcije

Slika 10. Vrijeme potrebno za otkrivanje kriminalnih radnji

Preporučene kontrole: ažuriranje pretraživača, onemogućiti korišćenje Jave u pretraživaču, korišćenje dvostepene autentifikacije i slično.

- **Card skimmers**
  Incidenti u kojima je fizički ugrađen uređaj koji čita podatke o platnim karticama (bankomati, benzinske pumpe, POS terminali itd.) koji eksportuju povjerljive podatke preko bluetooth-a i slično. U izvještaju se navodi da je od 130 incidentnih slučajeva, u svim slučajevima potvrđeno kompromitovanje podataka**.**

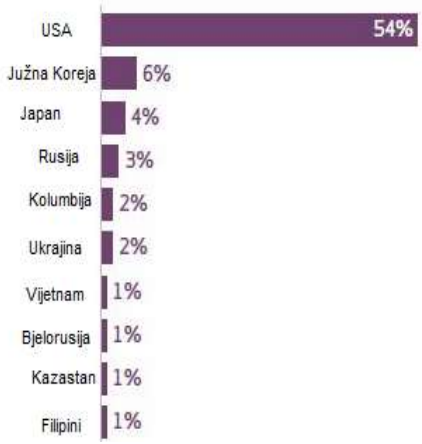


Slika 11. Prikaz porijekla aktera (skimera)

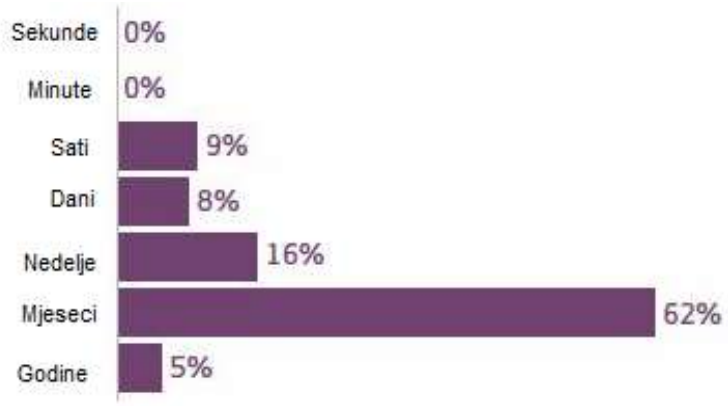
Preporučene kontrole: dizajnirati ili kupiti sigurnosne terminale, provjera neovlašćenih ometanja kamera, zaštitite PIN i slično.

- **DoS napadi**
  Napadi koji imaju za cilj da kompromituju dostupnost sistema i mreže. Od ukupno 1,187 incidenata nijedan nije potvrdio kompromitovanje podataka.
  Preporučene kontrole: serveri i servisi trebaju biti isključeni kada nisu u upotrebi, izolovati važnu imovinu(servere i servise) i slično.

- **Sajber špijunaža**
  Incidenti u ovoj kategoriji podrazumijevaju neovlašćeni mrežni pristup povezan sa državom, a čiji je glavni motiv – špijunaža. Od ukupno 511 incidenata, u 306 je potvrđeno kompromitovanje podataka.



Slika 12. Države pogođene sajber.špij.



Slika 13. Vrijeme potrebno za otkrivanje sajber. špij.

Preporučene kontrole: ažuriranje antivirusa, obuka korisnika, podizanje svjesnosti, čuvati logove, segmentirati mrežu itd.

Sajber prijetnje u Crnoj Gori

Podaci zavoda za statistiku

Kako bi stvorili što bolju sliku o crnogorskom sajber prostoru, veoma je bitno sagledati statističke podatke upotrebe informaciono-komunikacionih tehnologija u Crnoj Gori. Istraživanjem o upotrebi informaciono-komunikacionih tehnologija u Crnoj Gori, koje je sproveo Zavod za statistiku Crne Gore 2014.godine, dobijeni su sljedeći rezultati:

Domaćinstva:

- 53,7% ima pristup personalnom računaru (PC),
- 37,9% domaćinstava koristi laptop,
- 93,6% ima mobilni telefon.

U Crnoj Gori, 63,6% 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) – 75,1%, domaćinstava i prenosivi računar (laptop, netbook, tablet) – 57,6%. Pored navedenih uređaja za pristup Internetu se koriste i mobilni uređaji - 38,5%, smart TV, igračke konzole (play station) itd.

Privredni subjekti:

U Crnoj Gori 93,9% anketiranih preduzeća je izjavilo da je koristilo računare u svom poslovanju.

Kada je riječ o Internetu, istraživanje je pokazalo da je 98,1% preduzeća, koja su koristila računar, imalo pristup Internetu. Od preduzeća koja su imala pristup Internetu, 73,3% je odgovorilo da su imala Web Site/Home Page, što je 10,0% više u odnosu na prethodnu godinu.

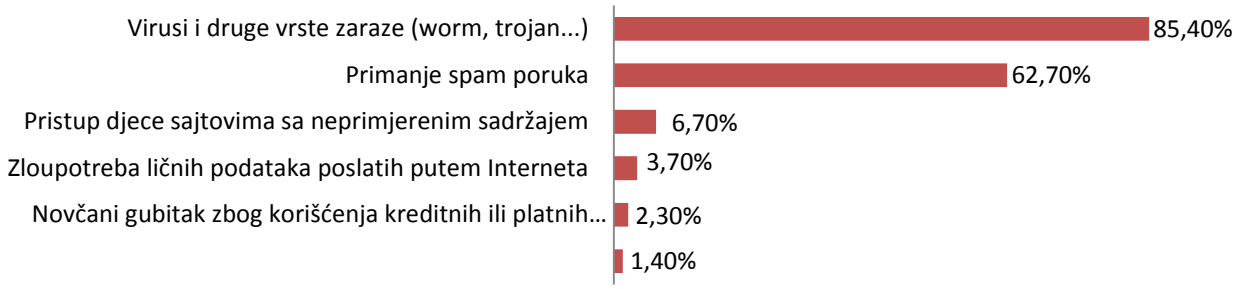
Prema rezultatima istraživanja 68,4% preduzeća (koja su koristila računar u svom poslovanju) je svojim zaposlenim omogućavalo daljinski pristup e-mail sistemu, dokumentima ili aplikacijama preduzeća.

Od preduzeća koja koriste računar u svom poslovanju, 37,7% je odgovorilo da zapošljava IKT/IT stručnjake koji imaju sposobnost da razvijaju, održavaju, upravljaju IKT ili IT sistemima i aplikacijama, što predstavlja rast od 16,9% u odnosu na 2012. godinu.

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

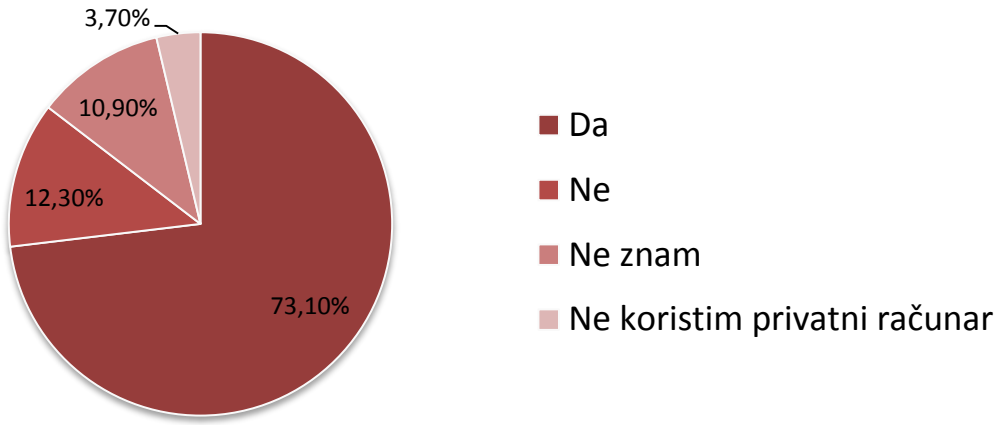
Domaćinstva:

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:



Slika 14.

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:



Slika 15.

Privredni subjekti:

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.

Iskustva nacionalnog CIRT-a

Statistika govori da globalni trendovi pokazuju ubrzano povećanje sajber napada. Sajber napadi, koji u početku predstavljaju samo manje smetnje, pretvaraju se u mnogo opasnije napade, motivisani novcem, političkim stvarima, a u najgorim slučajevima čak i sajber terorizmom.

Ministarstvo za informaciono društvo i telekomunikacije je prilikom formiranja CIRT tima, u saradnji sa ekspertima iz Malezije, pripremilo Izvještaj o procjeni stanja u sajber prostoru Crne Gore. Ovaj dokument sadrži izvještaj o aktivnostima, sprovedenim od strane ITU/IMPACT-a u Crnoj Gori, kako bi se sagledala kompletna analiza situacije u sajber prostoru. Za potrebe izvještaja, eksperti su konsultovali više različitih izvora u zemlji i sproveli mnogobrojna istraživanja kako bi prikupili što više informacija. Procjena o spremnosti pokazala je da Crna Gora nije imuna na razne vrste opasnosti u sajber prostoru, sa kojima su suočene razvijene zemlje, kao ni zemlje u razvoju.

U sklopu svojih svakodnevnih aktivnosti CIRT je zadužen za uspješno rješavanje prijavljenih incidenata. Incidenti se prijavljuju putem web sajta www.cirt.me.

Na nacionalnom nivou, CIRT ima odličnu saradnju sa ključnim državnim institucijama i nadležnim agencijama koje su prepoznate kao garanti sajber bezbjednosti pa u određenim slučajevima koordinišemo međusobne aktivnosti. (Uprava policije, tužilaštvo, nadležne agencije)

U zavisnosti od težine i opsega incidenta, neki od incidenata su zahtijevali prekograničnu saradnju i razmjenu informacija sa raznim organizacijama kao što su:

- CERT Bugarske, CERT Bulgaria;
- CERT Francuske, CERT-FR;
- CERT Hrvatske, HR-CERT;
- CERT Indije, CERT-IN;
- CERT Italije, CERT Pubblica Amministrazione;
- CERT Japana, JPCERT/CC;
- CERT Njemačke, CERT-Bund;
- CERT Slovenije, SI-CERT;
- CERT Sjedinjenih Američkih Država, US-CERT;
- Društvene mreže (Facebook, Skype, Twitter i sl);
- NATO;

Na međunarodnom nivou dobijamo informacije i podatke vezane za potencijalne napade, propuste i slično, od organizacija kao što su: FIRST, IMPACT, ITU, ENISA, Trusted Introducer.

Međunarnodna saradnja je od ključne važnosti za sajber sigurnost svake zemlje. Incidenti se u ovom prostoru ne dešavaju u granicama država, već su to uvijek globalni incidenti. Kako bi suzbili globalne prijetnje, potrebna je konstantna razmjena podataka i brzo djelovanje. Bez relevantnih podataka iz inostranstva u većini slučajeva ne bismo detektovali neke napade koji dolaze iz naše zemlje, ali na osnovu tih prijava mi uspjevamo da djelujemo.

Analizom trenutnog stanja, utvrđeno je da se sve više novih usluga i servisa nudi putem Interneta i da je sve veći broj prijavljenih sajber bezbjednosnih incidenata, kao što su distribuirani napadi uskraćivanja usluga - DDOS napadi, „hakovanje“(eng. hacking – neovlašćeni pristup računarskom sistemu), napadi na državne sajtove, phishing napadi i drugi.

Na osnovu toga, možemo vidjeti da su računarski sistemi i korisnici u Crnoj Gori izloženi većini sajber opasnosti i napada koje pogađaju ostatak svijeta. Ovo uključuje maliciozne programe, elektronske prevare, izmjene naslovnih web stranica i “hakovanje” elektronske pošte.

U periodu od osnivanja CIRT-a, od 2011-2014. godine, napadači su izmijenili ili preuzeli kontrolu nad više naslovnih web stranica crnogorskih institucija. Dogodilo se više napada na informatičku infrastrukturu, na servise provajdera Interneta, kao i na bankarski sektor. Primijećen je 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. 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.

U posmatranom četvorogodišnjem periodu, 2011. godina se ističe kao godina sa najmanjim brojem incidenata. Evidentno je da se iz godine u godinu, broj incidenata povećavao. Najveći broj prijavljenih incidenata je u tekućoj godini.

Analizom statističkih podataka nesumnjivo se utvrđuje da je zloupotreba profila na društvenim mrežama najčešći problem sa kojim se susrijeću građani Crne Gore. Ovo saznanje ukazuje na opasnosti kojima se korisnici izlažu prilikom postavljanja ličnih podataka i sadržaja na Internet. Na drugom mjestu su napadi na web portale državnih organa, organa državne uprave i pravnih lica (web defacement, DoS napad, trojanac i slično). Nije zanemarljiv ni broj bankarskih prevara i *phishing* napada. Ova vrsta kriminala je trenutno najpopularnija u Crnoj Gori, a i na čitavom Balkanu. Poslednji primjeri sajber incidenata pokazuju da je veliki broj slučajeva u kojima lažne web stranice inostranih banaka egzistiraju na crnogorskim sajtovima i da sve više novčanih transakcija odlazi u ruke hakera na drugom kraju svijeta.

Kada su u pitanju najveći i najpoznatiji incidenti koji su se dogodili u svijetu, veoma je važno napomenuti da su se neki od njih proširili i imali efekta na području Crne Gore. Među incidentima se ističe pojava trojanca, “MiniDuke” koji je kao metu imao državne

institucije na internacionalnom nivou, zatim slučaj sajber špijunaže “Red October” gdje je jedna od pogođenih IP adresa bila iz Crne Gore, pojava crva “Conficker” i slično, gdje je CIRT, na osnovu pravovremene dojave od partnerskih organizacija, "izolovao” IP adrese, koje su se nalazile u sajber prostoru Crne Gore.

Zaključak

Prema izvještaju Centra za strateška i međunarodna istraživanja, procjenjuje se da godišnja šteta od sajber kriminala, na globalnom nivou, iznosi više od 400 milijardi eura. Na osnovu ovih podataka možemo zaključiti da su posljedice sajber kriminala, koji ne zaobilazi ni Crnu Goru, teške i dalekosežne.

Na osnovu iskustava CIRT-a, vidimo da su globalne sajber prijetnje itekako prisutne u Crnoj Gori. Takođe, vidimo da se statistika najvećih globalnih sajber prijetnji ne razlikuje u velikoj mjeri u odnosu na crnogorski sajber prostor.

Imajući u vidu rezultate analize, jasno je da je u budućnosti neophodno posvetiti više pažnje ovoj tematici. U nastavku su navedene neke od aktivnosti koje je neophodno sprovesti kako bi povećali nivo bezbjednosti.

Savjeti za državne organe i privatni sektor:

- Web portali državnih institucija i kompanija iz privatnog sektora su česta meta haktivista, pa je potrebno posvetiti više pažnje pravilnoj izradi web stranica i zaštiti od mogućih napada.

- Jedna od najvećih globalnih prijetnji je spam, zbog čega je neophodno implementirati antispam rješenja. Takođe, dobra praksa je i konfigurisati mail sarver da blokira priloge (attachment) koji se najčešće koriste za širenje virusa, kao što su .VBS, .BAT, .EXE, .PIF i .SCR fajlovi.

- Kada su u pitanju državni organi i privatni sektor, antivirusna zaštita nije dovoljna. Naravno da je neophodna, ali su isto tako neophodni i alati za monitoring, ažuriranje softvera, uklanjanje ranjivosti, zaštita od DDoS i ciljanih napada, kao i zaštita mobilnih uređaja koji se koriste u poslovne svrhe.

- Svi uređaji koji se koriste u mreži moraju imati adekvatnu zaštitu, uključujući i mobilne uređaje.

- Forsirati kompleksnu password politiku.

- Kreirati i održavati regularan backup kritičnih sistema.

- Sajber incidenti mogu dovesti do ozbiljnih finansijskih gubitaka i urušavanja ugleda. Ovi gubici su u većini slučajeva veći od same investicije u IT bezbjednosna rješenja, pa je samim tim veoma bitno ulagati u IT bezbjednost.

- Razvoj i implementacija bezbjednosnih pravilnika je još jedan od ključnih djelova sveukupne bezbjednosti. U većini incidenata u kojima je došlo do curenja

povjerljivih podataka, istragom je utvrđeno da zaposleni nisu ispoštovali bezbjednosne pravilnike.

- Kreirati procedure za odgovor na sajber incidente.
- Edukovati zaposlene o osnovama sajber bezbjednosti.
- Ojačati institucionalnu saradnju i obuku po pitanju sajber prijetnji.

Savjeti za pojedinačne korisnike:

- Krađa identiteta je jedan od najčešće prijavljivanih incidenata u Crnoj Gori, pa je neophodna edukacija građana o zaštiti svog identiteta na Internetu, uključujući zaštitu naloga na društvenim mrežama.
- Koristiti kompletna rješenja za bezbjednost na Internetu koja uključuju antivirus, firewall, zaštitu Web browsera, a po potrebi i alate za roditeljsku kontrolu.
- Redovno ažurirajte softverska rješenja koja koristite. Zastarjele verzije su ranjivije na napade.
- Koristiti kompleksne lozinke koje sadrže mala i velika slova, brojeve i specijalne karaktere. Ne koristiti riječi koje se mogu naći u riječniku.
- Ne otvarati email i ne gledati prilog ukoliko je od nepoznatog pošiljaoca i ukoliko ne očekujete taj email.
- Treba biti oprezan pri otvaranju URL linkova koji se pojavljuju na društvenim mrežama ili u email-ovima, pa čak i ako dolaze od prijatelja kojima vjerujete.
- Biti oprezan kod pop-up prozora koji nude besplatne alate za media plejere, antivirusnu zaštitu i slično.