Vlada Crne Gore
Ministarstvo javne uprave

Strategija sajber bezbjednosti Crne Gore 2018-2021

Podgorica, decembar 2017. godine

SADRŽAJ

1. Uvodna razmatranja

1. Uvodna razmatranja

Zbog konstantnog rasta broja usluga koje javni i privatni sektor pružaju putem Interneta, kako građanima, tako i drugim pravnim subjektima, bezbjedan sajber prostor Crne Gore postaje jedan od nacionalnih prioriteta.

Pametni telefoni, društvene mreže, sistemi za industrijsku kontrolu proizvodnje, brojni medicinski uređaji kontrolisani od strane informacionih sistema, samo su neki od primjera stavljanja tehnologija u upotrebu, odnosno benefita koje one pružaju.

Procjena je da trenutno ima oko 8 milijardi inter-konektovanih uređaja u svijetu. Predviđa se da će do 2020. godine broj uređaja premašiti cifru od 20 milijardi, što svjedoči o stepenu integracije fizičkih sistema sa kompjuterskim sistemima koje će za posljedicu imati veću efikasnost, preciznost, veći ekonomski benefit, ali i ozbiljnije negativne posljedice u slučaju sajber napada.

Imajući u vidu sve veću integraciju sajber sistema i fizičkih sistema, te negativnih posljedica koje kompromitovani sajber sistem može prouzrokovati, sajber bezbjednost i njena izgrađena nacionalna, regionalna i međunarodna arhitektura imaju krucijalnu ulogu.

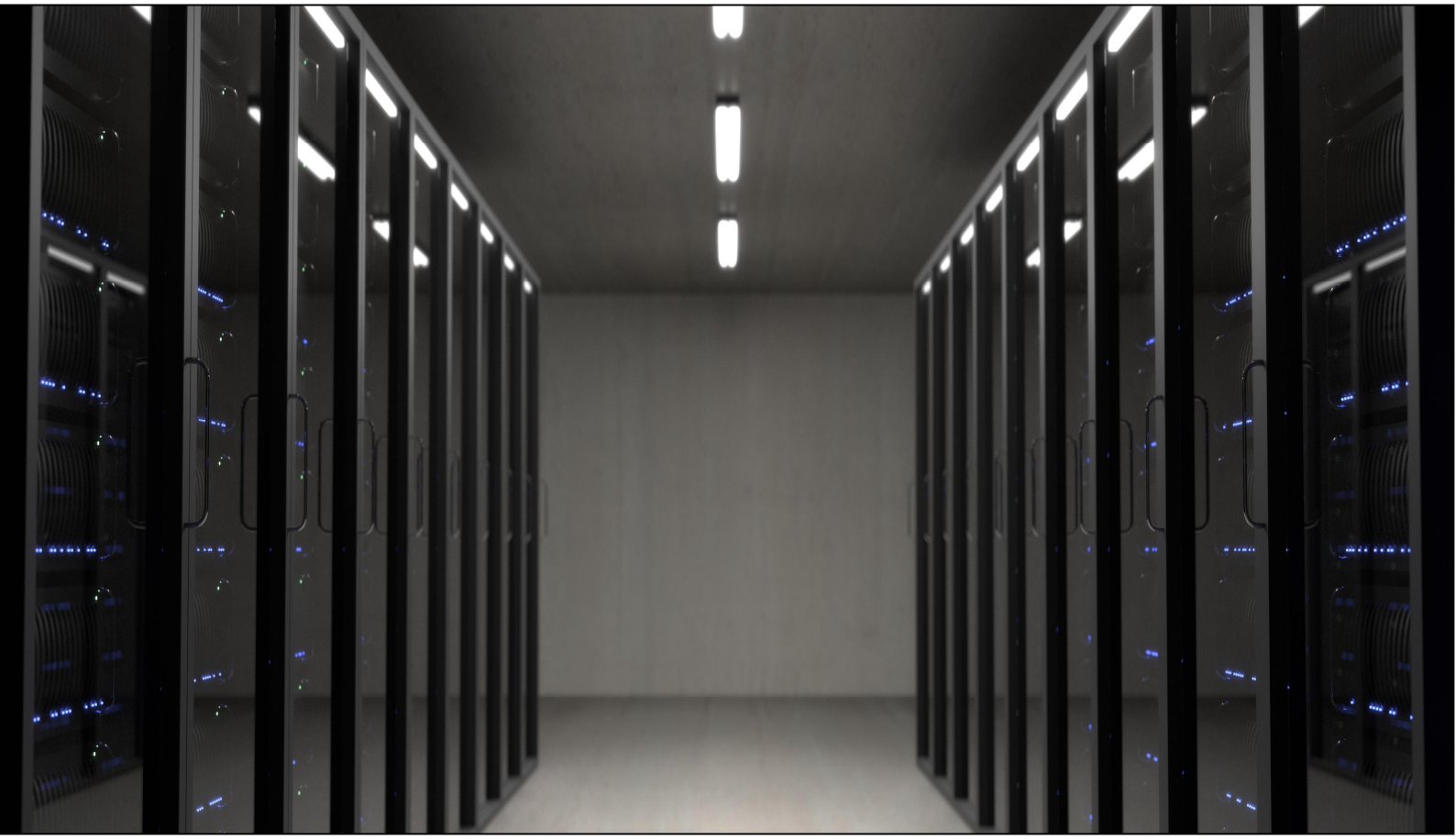
Ubrzan razvoj interkonektovanih, inovativnih tehnologija mora da prati i brz razvoj sajber-bezbjednosnih rješenja, odnosno zaštite od širokog spektra prijetnji i to svakako predstavlja izazov na koji svi, udruženim snagama, moramo da odgovorimo.

Nesumnjivo je da sajber bezbjednost predstavlja izazov savremenog doba i kao takav nije zaobišao ni Crnu Goru. Svjedoci smo sve većeg broja sajber incidenata koji pogađaju Crnu Goru, kroz nedavne ransomware kampanje, DDoS napade na državnu infrastrukturu, razne prevare putem Interneta, i sl. Broj ovih sajber incidenata se značajno povećava iz godine u godinu.

Moramo biti svjesni da prijetnje po IK infrastrukturu koje mogu da ugroze dostupnost, privatnost i integritet istih, takođe, mogu da utiču na funkcionisanje društva u cjelini. Države, međunarodne organizacije, sigurnosne kompanije i razni drugi entiteti konstantno razvijaju i implementiraju nove sigurnosne mehanizme, međutim, paralelno se odigrava proces u kojem sajber kriminalci pronalaze inovativne i sofisticirane tehnike za njihovo prevazilaženje.

U pogledu razvoja informacionih tehnologija i sajber bezbjednosti Crna Gora se na osnovu izvještaja Ujedinjenih nacija, odnosno Međunarodne unije za telekomunikacije (ITU) pod nazivom "Globalni sajber bezbjednosni indeks[1] 2017", nalazi na 71. mjestu od 193. države članice. Međutim, u uslovima svakodnevnih pojava novih prijetnji i naši napori kada je u pitanju sajber bezbjednost moraju pratiti takav tempo.

[1] Globalni sajber bezbjednosni indeks za 2017. godinu. Link: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf



2. Savremeni rizici, prijetnje i izazovi

2. Savremeni rizici, prijetnje i izazovi

Konstantan napredak informacionih tehnologija i proširenje sajber prostora u velikoj mjeri podstiče ekonomski i socijalni napredak svake države svijeta. Informaciona bezbjednost predstavlja zajednički interes kompletnog čovječanstva i odnosi se na globalni mir i razvoj, kao i na nacionalnu bezbjednost svih država. Međutim, ova prednost sa sobom nosi i nove bezbjednosne rizike i izazove.

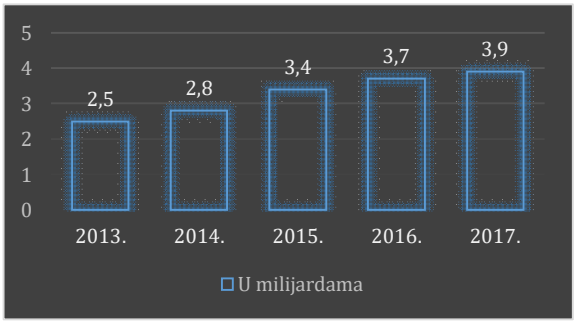
Rizici i izazovi sa kojima se suočava veliki broj država su brojni. Između ostalog, porast broja informacionih sistema i tehnologija uslovio je uspostavljanje novih memorijskih okruženja (Cloud Storage), što svakako predstavlja veliki izazov i predmet je posebnih analiza. Takođe, evidentan je porast broja malicioznih programa za mobilne uređaje.

Prema istraživanju koje je predstavila kompanija Symantec u aprilu 2017. godine[2], u 2016. godini je detektovano oko 18,4 miliona malicioznih programa, što je za 105% više u odnosu na 2015. godinu (9 miliona). U 2014. godini je detektovano približno 3,6 miliona malvera.

Revolucija novih tehnologija

Internet revolucija sa sobom nosi niz izuzetno korisnih mogućnosti, pa ne čudi činjenica da je evidentan veliki porast broja korisnika svakog dana.

Interesantan je podatak da je od početka sprovođenja prethodne Strategije sajber bezbjednosti u Crnoj Gori (2013. godine) broj korisnika interneta na globalnom nivou porastao sa 2,5 milijarde na 3,9 milijardi (do juna 2017. godine)[3].



Grafikon – *Penetracija internet korisnika na globalnom nivou u periodu 2013-2017. godine*

U literaturi možemo naići na formulaciju „*proliferacija sajber tehnologija*". Ovaj pojam se odnosi na raščlanjivanje ili množenje tehnologija koje povezivanjem na globalnu mrežu takođe postaju dio sajber prostora.

Jedan od izvora proliferacije sajber rizika predstavlja "Internet stvari" (eng. *Internet of Things – IoT*), pojam koji prvi put definiše Kevin Ashton, osnivač Auto-ID Centra MIT-a, u svom izlaganju o novim mogućnostima RFID-a u lancu

[2] Symantec Internet Security Report vol. 22 - https://www.symantec.com/content/dam/symantec/docs/reports/gistr22-government-report.pdf

[3] Link: http://www.internetworldstats.com/emarketing.htm

snabdijevanja kompanije Procter & Gamble 1999. godine.[4]

IoT predstavlja skup uređaja, vozila, uređaja za domaćinstvo, kao i drugih objekata sa ugrađenom elektronikom, softverom, sanzorima i sl. povezanih na zajedničku mrežu. Uzimajući u obzir činjenicu da se povezivanjem prethodno pomenutih objekata omogućava nesmetana komunikacija, bilježenje informacija i razmjena podataka, zabrinutost u informatičkom svijetu je sasvim opravdana. Samim tim, ovaj pojam predstavlja jedan od vodećih bezbjednosnih pitanja u svijetu.

Pojam koji obuhvata veći domen se zove "Internet svega" (eng. *Internet of Everything* – IoE) i prvi put je definisan od strane kompanije CISCO u okviru studije pod nazivom "Internet of Everything Value Index" iz 2013. godine[5].

"Ulazimo u četvrtu generaciju interneta. U narednih 10 godina ćemo vidjeti da će se kompetitivnost kompanija mjeriti po tome koliko dobro razumiju IoE koncept i koliko ga primjenjuju."

Michael Ganser
Viši potpredsjednik kompanije CISCO
za region centralne Evrope

IoE predstavlja inteligentnu mrežu ljudi, procesa, podataka i stvari. Preciznije, temelji se na IoT, dodajući mrežnu inteligenciju koja omogućava efikasnu upotrebu telefonske, video i komunikacije podataka kroz istu mrežu (konvergenciju), automatizaciju ili poboljšanje procesa uz potencijalnu sinhronizaciju podataka u realnom vremenu (orkestracija), kao i vidljivost u različitim sistemima.

Sa druge strane, obilje različitih mogućnosti nosi sa sobom prijetnje koje u velikoj mjeri mogu ostaviti štetne posljedice.

Prema studiji koju je predstavila jedna od vodećih britanskih i svjetskih kompanija iz oblasti istraživanja u 2017. godini, IHS technology, preko interneta je povezano više od 20 milijardi uređaja. Predviđa se da će do kraja 2020. godine biti najmanje 30 milijardi, dok će do 2025. godine brojka preći nevjerovatnih 75 milijardi[6].

Takva ekspanzija uređaja će svakako donijeti nove mogućnosti, ali i otvoriti novi prostor za djelovanje zlonamjernih pojedinaca ili grupa, iz razloga što u većini slučajeva uređaji nijesu dizajnirani po standardima za online bezbjednost.

Prijetnje i rizici u sajber prostoru

Uzimajući u obzir krajnji cilj sajber aktivnosti, prijetnje se mogu svrstati u dvije osnovne kategorije:

- **sajber napadi** (*napadi od strane dugih država, haktivizam, špijunaža, sabotaža*), **sajber terorizam i sajber kriminal** (*stvaranje terorističkih organizacija, napadi od strane individualaca ili grupa, organizovani kriminal*), **sajber ratovanje**,

[4] RFID Journal – "That 'Internet of Things' Thing": http://www.rfidjournal.com/articles/view?4986
[5] Link: https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1209280
[6] IHS Technology – IoT platforms: enabling the Internet of Things: https://cdn.ihs.com/www/pdf/enabling-IOT.pdf

- **rizici uslovljeni ljudskom greškom ili prirodnim fenomenima**.

Ilustracija – *Prijetnje i rizici u sajber prostoru*

Sajber napadi

Pod sajber napadima se mogu podvesti brojne aktivnosti. U velikom broju slučajeva napadi se izvode u svrhu špijunaže i sabotaže.

Špijunaža se odnosi na neprimjetno praćenje i prikupljanje informacija i povjerljivih podataka o ličnosti ili kompaniji upotrebom različitih softvera i servisa, koji se u konačnom mogu javno predstaviti, najčešće putem sredstava javnog informisanja. Obično se aktivnosti sprovode koristeći metod koji se naziva "backdoor", koji može predstavljati poseban softver ili biti inkorporiran kao programski kod u firmware nekog mrežnog uređaja i tako dostavljati informacije napadaču.

Sabotažom se postižu određeni ciljevi, najčešće političke prirode. Na taj način se namjerno ometaju procesi institucionalnog rada ili vojnog djelovanja i omogućava svrgavanje ili preuzimanje kontrole i komandovanja. Najčešći primjeri sabotiranja su sprovedeni korišćenjem botnet-ova za ostvarivanje DDoS/DoS napada.

Kompanije Kaspersky Lab i B2B International su u toku 2016. godine anketirale oko 4.000 kompanija iz ukupno 25 zemalja koje su bile pogođene nekim od DDoS napada.[7] Oko 40% kompanija se izjasnilo da vjeruju da je do napada došlo od strane konkurencije, njih 20% okrivljuju strane vlade i tajne službe, dok je 20% izrazilo sumnju da su napade izvršili bivši zaposleni radnici.

Drugi problem se odnosi na **sajber kriminal** i **haktivizam**. U svijetu je evidentan porast broja malicioznog softvera, koji se distribuira na različite načine. Pokretanjem ovakvog softvera omogućava se krađa osjetljivih podataka, pribavljanje novčane koristi, prekid rada servisa i eventualno uništenje podataka i uređaja.

Haktivizam predstavlja radnju hakovanja ili ulaska u računarski sistem, iz političkih ili socijalnih razloga.

Takođe, internet penetracija omogućava adekvatno djelovanje aktera **sajber terorizma**. U današnje vrijeme je mnogo lakše stvarati terorističke organizacije, manje organizovane grupe ili angažovati individualce koji će u ime određenih interesa posjedovati veliku moć da prouzrokuju što je moguće veću štetu, koristeći savremene internet tehnologije. S tim u vezi, organizuju se brojni napadi na kritičnu informacionu infrastrukturu država, što prerasta u model **sajber ratovanja**.

[7] Kaspersky Lab Finds Businesses are Unclear on How to Combat Targeted Attacks and DDoS: https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-finds-businesses-are-unclear-on-how-to-combat-targeted-attacks-and-ddos

Napadom i/ili uništenjem kritične informatičke infrastrukture postižu se ciljevi prekida ili kompletnog gašenja vitalnih državnih ili vojnih komunikacija, što prouzrokuje određene konsekvence po civilnu populaciju. Na primjer, napadom na industrijske kontrolne sisteme u elektro-energetskom sistemu može doći do prekida proizvodnje i/ili distribucije električne energije za stanovništvo, što prouzrokuje brojne probleme. Takođe, napadom na informacione sisteme u zdravstvenom sektoru može se prouzrokovati narušavanje zdravlja ljudi, kroz eventualno modifikovanje paramatara na uređajima preko kojih pacijenti internetom komuniciraju sa sistemom u zdravstavnoj ustanovi.

Uz sve navedeno, potrebno je napomenuti da veliki izazov takođe predstavlja i činjenica da su u današnje vrijeme u velikoj mjeri dostupna online uputstva koja se tiču organizacije sajber napada, po modelu "*know-how to launch cyber attacks*".

Rizici uslovljeni prirodnim nepogodama ili ljudskom greškom

Kompanija IBM je u svojoj ekspertizi "2014 Cyber Security Intelligence Index" predstavila krajnje intrigantan podatak koji govori da je 95% svih bezbjednosnih incidenata uslovljeno faktorom ljudske greške.

Mnogi uspješni napadi su sprovodeni tako što su napadači koristili ljudske slabosti i raznim oblicima zastrašivanja od zaposlenih pravili insajdere, koji su nevoljno omogućavali pristup tajnim podacima.

Nasuprot tome, konstantni rizici koje je teško predvidjeti, a sa kojima se bori kompletno čovječanstvo su uzrokovani prirodnim nepogodama, kao što su: zemljotresi, poplave i uragani. Veliko fizičko oštećenje mogu prouzrokovati i požari, ekstremno visoke temperature i udari groma, što takođe može dovesti do gubitka podataka.

Drugi značajni izazovi

Izazovi koji se odnose na unutrašnja pitanja jedne države zanačajni su podjednako kao i prethodno opisani rizici i prijetnje. Tačnije, predstavljaju jedan od važnih preduslova za adekvatnu sajber zaštitu.

Prepoznata je potreba za daljim ulaganjem sredstava u pravcu jačanja resursa, ekspertize i kontinuiranog progresa u oblasti proaktivnog djelovanja u okviru sajber prostora Crne Gore. U velikom broju zemalja i međunarodnih organizacija, kao što su NATO i EU, sajber bezbjednost predstavlja jedan od glavnih prioriteta, pa je tako i ovaj problem definisan u odgovarajućim strategijama i konceptima sajber bezbjednosti.

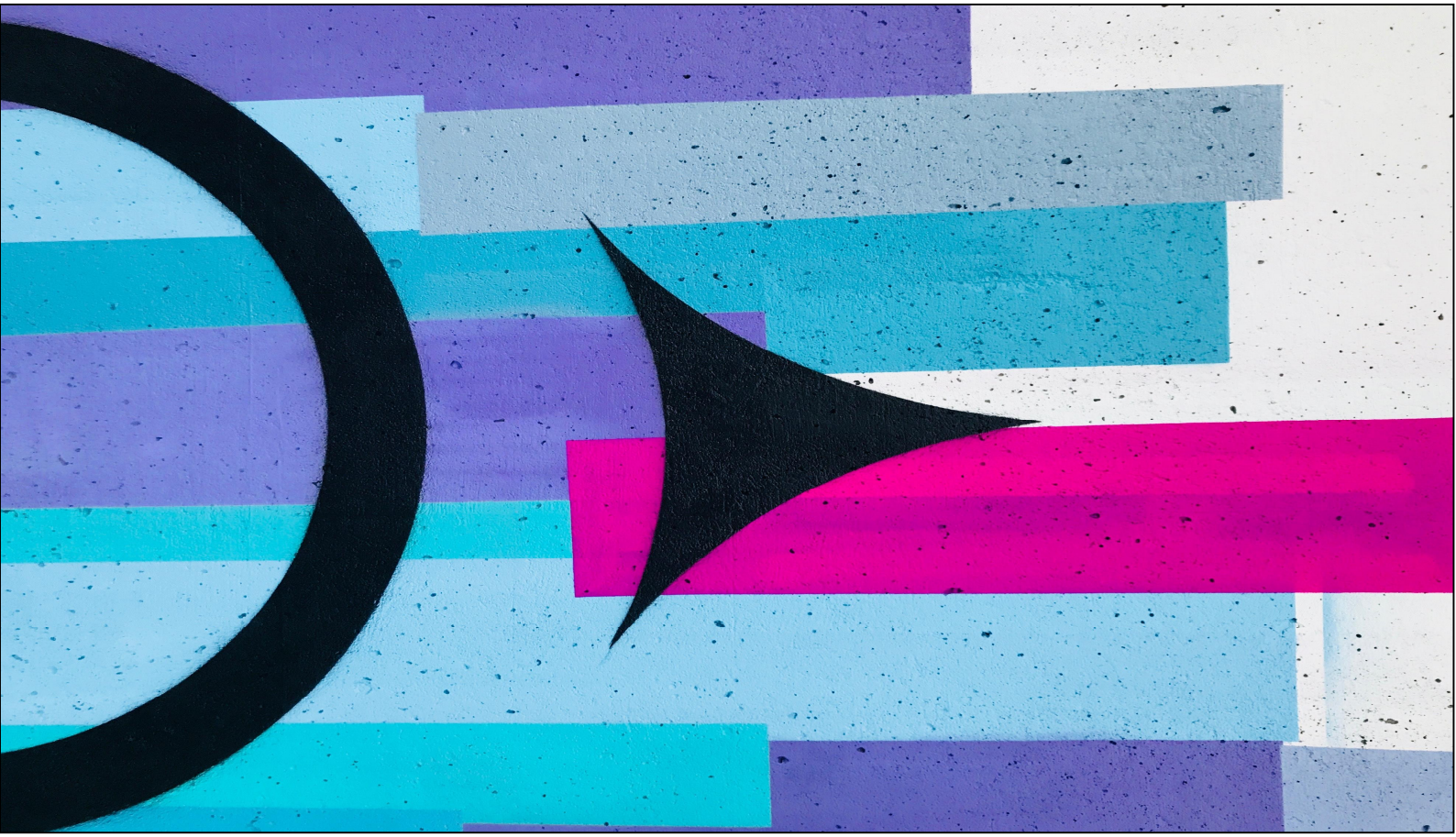
Uz prethodno navedeno, **ograničenost pravnog okvira** u ovoj oblasti prouzrokuje poteškoće u sprovođenju procedura. Naime, ostaje izazov da se sajber napadi na jednu državu označe kao digitalni "oružani napadi". Iz tog razloga izostaje adekvatna **kooperacija na internacionalnom nivou**, dok je i

uloga međunarodnih organizacija takođe veoma ograničena.

Neadekvatna **komunikacija i saradnja između javnog i privatnog sektora** prouzrokuje u velikoj mjeri nedostatak povjerenja građana u institucije i kompanije koje se bave elektronskim poslovanjem. Sa druge strane, **nedovoljna digitalna pismenost krajnjih korisnika** i **zanemarivanje poštovanja dobrih praksi** prilikom korišćenja uređaja za komunikaciju predstavlja poseban izazov. Razlog za prethodno navedeni problem je **nedovoljno podignuta svijest kod stanovništva** o problemu sajber bezbjednosti u globalu.

Konačno, veliki izazov država predstavlja **mali broj eksperata** koji bi bili u mogućnosti da konstantno učestvuju u domenu sajber bezbjednosti i adekvatno sprovode reforme.

Prateći najbolje sigurnosne prakse, jedan od izazova predstavlja i **jasno razdvajanje funkcija administracije i upravljanja informacionim sistemima od funkcije upravljanja bezbjednošću** tih sistema. U slučajevima ograničenih ljudskih resursa, u pojedinim institucijama funkcije bezbjednosti i administracije se poklapaju. Ova činjenica direktno prouzrokuje smanjenje nivoa bezbjednosti sistema iz razloga što ne postoji drugostepena kontrola nad administratorima, već oni sami obavljaju i funkciju bezbjednosti svoje institucije.



3. Retrospektiva

3. Retrospektiva: od prve Strategije sajber bezbjednosti do danas

Strategija sajber bezbjednosti Crne Gore 2018-2021 predstavlja strategiju kontinuiteta u odnosu na prethodnu, čiji se životni ciklus završava krajem 2017. godine.

Polaznu osnovu za aktivnosti koje će biti preduzete na planu definisanja i implementacije Strategije sajber bezbjednosti Crne Gore 2013-2017 činili su, u zakonodavnom smislu - Zakon o informacionoj bezbjednosti ("Službeni list Crne Gore", br. 014/10), dok u institucionalnom smislu – Direkcija za zaštitu od računarskih i bezbjednosnih incidenata na internetu – CIRT, koja je funkcionisala u okviru tadašnjeg Ministarstva za informaciono društvo i telekomunikacije, a danas organizaciono pripada novoformiranom Ministarstvu javne uprave 41. Vlade Crne Gore, sa zadatkom da omogući rano otkrivanje sajber prijetnji i incidenata i adekvatno reaguje i odgovori na iste.

Prva Strategija sajber bezbjednosti Crne Gore donešena je 2013. godine za period do 2017. godine i sadrži sedam ključnih strateških ciljeva:

1) Definisanje institucionalne i organizacione strukture na polju sajber bezbjednosti u državi;
2) Zaštita kritične informatičke infrastrukture u Crnoj Gori;
3) Jačanje kapaciteta državnih organa za sprovođenje zakona;
4) Odgovor na incidentne situacije;
5) Definisanje uloge Ministarstva odbrane i Vojske Crne Gore u sajber prostoru;
6) Partnerstvo javnog i privatnog sektora;
7) Podizanje nivoa svijesti u društvu i zaštita na Internetu.

Realizacija navedenih strateških ciljeva bila je detaljnije definisana kroz dva akciona plana za implementaciju Strategije. Uvidom u status njihove realizacije evidentna je intenzivna aktivnost nadležnih organa u ispunjavanju zacrtanih strateških ciljeva, što je rezultiralo uspješnom implementacijom dijela aktivnosti prepoznatih akcionim planovima.

U nastavku poglavlja, detaljno su opisane aktivnosti sprovedene u cilju realizacije glavnih strateških ciljeva Strategije sajber bezbjednosti Crne Gore 2013-2017, kao i aktivnosti koje nisu sprovedene na zadovoljavajućem nivou, i koje će biti tretirane Strategijom sajber bezbjednosti Crne Gore 2018-2021.

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

Kroz ovaj strateški cilj, prepoznata je potreba da u okviru državne uprave postoji jasna organizaciona hijerarhija, sa definisanim nadležnostima, koja će obezbijediti efikasno upravljanje sajber bezbjednošću u Crnoj Gori. Sledeće institucije su prepoznate za nosioce sajber bezbjednosti Crne Gore:

- Ministarstvo javne uprave u okviru kojeg funkcioniše nacionalni CIRT tim;
- Agencija za nacionalnu bezbjednost;
- Ministarstvo odbrane/ Vojska Crne Gore;
- Ministarstvo unutrašnjih poslova/ Uprava policije;

- Ministarstvo pravde;
- Ministarstvo prosvjete;
- Direkcija za zaštitu tajnih podataka.

U okviru pratećeg dvogodišnjeg akcionog plana za implementaciju Strategije, predviđeno je formiranje Savjeta za infomacionu bezbjednost, koji je obrazovan na 29. sjednici Vlade, 08. juna 2017. godine.

Dodatno, u cilju snaženja sajber infrastrukture na lokalnom nivou, Strategijom sajber bezbijednosti Crne Gore 2013-2017 predviđeno je formiranje lokalnih CIRT timova ili određivanje kontakt osoba u svim državnim organima. Kreirano je 31 lokalnih timova koji su zaduženi za saradnju sa članovima nacionalnog CIRT-a vezano za pitanja zaštite od računarskih bezbjednosnih incidenata na internetu.

Stepen realizacije: Evidentno je da se u državnim organima sve više pažnje posvjećuje sajber bezbjednosti i da su institucije u dobroj mjeri prepoznale svoju ulogu u sajber prostoru. Dalje aktivnosti na planu kompletiranja liste lokalnih CIRT timova ii određivanja kontakt osoba za pitanja sajber bezbjednosti, biće predmet aktivnosti nadležnih institucija kroz Akcioni plan 2018-2019 koji će pratiti Strategiju sajber bezbjednosti Crne Gore 2018-2021.

2. Zaštita kritične informatičke infrastrukture u Crnoj Gori

U skladu sa zadatkom, tadašnje Ministarstvo za informaciono društvo i telekomunikacije 40. Vlade Crne Gore je izradilo Zakon o izmjenama i dopunama Zakona o informacionoj bezbjednosti ("Službeni list Crne Gore", br. 040/16) kojim je definisana kritična informatička infrastruktura (KII).

Kritičnu informatičku infrastrukturu čine informacioni sistemi čijim bi se prekidom rada ili uništenjem ugrozili život, zdravlje, bezbjednost građana i funkcionisanje države i od čijeg funkcionisanja zavisi vršenje djelatnosti od javnog interesa.

Vlada Crne Gore je na predlog tadašnjeg Ministarstva za informaciono društvo i telekomunikacije usvojila Metodologiju izbora kritične informatičke infrastrukture. Na osnovu Metodologije, Ministarstvo javne uprave koje je naslijedilo određene nadležnosti nekadašnjeg Ministarstva za informaciono društvo i telekomunikacije, je u saradnji sa drugim nadležnim institucijama definisalo listu kritične informatičke infrastrukture u Crnoj Gori, a u toku je i izrada Uredbe o mjerama za zaštitu KII.

Stepen realizacije: Početna lista kritične informatičke infrastrukture u Crnoj Gori je usvojena, međutim, treba imati u vidu da se lista mora redovno ažurirati. Nakon usvajanja Uredbe o mjerama za zaštitu KII, istu je neophodno i implementirati u saradnji sa vlasnicima KII.

3. Jačanje kapaciteta državnih organa za sprovođenje zakona;

U proteklom periodu Crna Gora je kroz legislativu i strateška dokumenta pratila ono što su glavni standardi, smjernice i preporuke EU i NATO-a na planu izgradnje kapaciteta u oblasti sajber bezbjednosti.

Legislativa u oblasti informacione bezbjednosti u značajnoj mjeri je

usaglašena sa pravnom tekovinom Evropske unije. Dodatno, 2016. godine usvojen je Zakon o izmjenama i dopunama Zakona o informacionoj bezbjednosti ("Službeni list Crne Gore", br. 040/16) kojim su predviđene dvije ključne aktivnosti: formiranje Savjeta za informacionu bezbjednost i zaštita kritične informatičke infrastrukture, koje su u skladu sa NIS Direktivom (2016/1148)[8].

Sa ciljem jačanja kapaciteta državnih organa za sprovođenje zakona, u Ministarstvu unutrašnjih poslova, formirana je Grupa za borbu protiv visokotehnološkog kriminala, koja je pozicionirana u Odsjeku za borbu protiv organizovanog kriminala i korupcije. U navedenoj Grupi sistematizovana su tri službenička mjesta koja se bave problematikom visokotehnološkog kriminala (klasičnim djelima kompjuterskog kriminala, dječijom pornografijom, zloupotrebom brojeva kreditnih kartica i zloupotrebom autorskih prava).

U Forenzičkom centru Uprave policije u Danilovgradu, od juna 2013. godine sistematizovana je grupa za ispitivanje informacionih tehnologija. Kad su u pitanju tehnički kapaciteti, pored alata za ispitavanje računara, izvršena je nabavka alata za ispitivanje mobilnih telefona.

Agencija za nacionalnu bezbjednost ulaže značajne napore u cilju stvaranja normativnih i operativnih mehanizama za borbu protiv sajber kriminala i špijunaže, koji uz terorizam i organizovani kriminal, postaje najveći bezbjednosni izazov današnjice. Agencija u kontinuitetu intenzivno radi na jačanju organizacionih i tehničkih kapaciteta u oblasti sajber bezbjednosti.

Služba za IKT Ministarstva pravde, u cilju jačanja otpornosti informacionih sistema, je u skladu sa zadacima iz Strategije sprovela niz aktivnosti, koje u velikoj mjeri smanjuju ranjivost postojećih sistema ministarstva u sajber prostoru.

Stepen realizacije: Iako su državni organi u proteklom periodu prepoznali potrebu za jačanjem svojih kapaciteta iz oblasti sajber bezbjednosti i sajber kriminala, neophodno je u kontinuitetu ulagati napore na planu daljeg unapređenja kapaciteta za sajber odbranu na nacionalnom nivou.

4. Odgovor na incidentne situacije

Analizom izvještaja o incidentnim situacijama u Crnoj Gori, koje CIRT izrađuje na godišnjem nivou, evidentan je trend rasta broja prijavljenih incidenata iz godine u godinu, kao i sve veća sofisticiranost samih napada.

Osnivanjem nacionalnog CIRT-a napravljen je krupan korak ka povećanju sposobnosti državnih organa da odgovore na sajber incidente koje pogađaju Crnu Goru. **Stepen realizacije:** CIRT je prepoznat kao centralna tačka za odgovor na incidentne situacije u Crnoj Gori, međutim, evidentan je nedostatak usko specijalizovanih kadrova kako bi se na ovaj izazov uspješno odgovorilo. Pored navedenog, za odgovor na incidentne situacije neophodno je realizovati i zadatke koji se odnose na kompletiranje liste lokalnih CIRT timova, kao i na

[8] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

obuke za usku specijalizaciju službenika iz oblasti sajber bezbjednosti.

5. Definisanje uloge Ministarstva odbrane i Vojske Crne Gore u sajber prostoru

Ministarstvo odbrane (MO) i Vojska Crne Gore (VCG) su u potpunosti nadležni za sajber prostor koji je kreiran unutar MO i VCG, i sarađuju sa nacionalnim CIRT-om u zaštiti sajber prostora Crne Gore.

Prihvaćeni su NATO ciljevi (E 6202 N) kojim su definisani kapaciteti koje MO i VCG trebaju da razviju u narednom periodu od 2 do 5 godina.

Stepen realizacije: MO i VCG imaju jasnu viziju svoje uloge u sajber prostoru. Za naredni period su planirane dalje aktivnosti kroz koje će se uloga MO i VCG dodatno osnažiti.

6. Partnerstvo javnog i privatnog sektora

Veliki dio kritične informatičke infrastrukture pripada privatnom sektoru. Zato je neophodno definisati jasnu saradnju sa privatnim sektorom na polju sajber bezbjednosti.

Kada je u pitanju privatni sektor, kreirano je sedam CIRT timova u okviru kompanija Crnogorski Telekom, Telenor, M:tel, Wireless Montenegro, Telemach, M-kabl i Societe Generale Montenegro Banka.

Jedan od najboljih primjera saradnje sa privatnim sektorom su aktivnosti koje su sprovedene na organizovanju zajedničkih promotivnih kampanja na temu zaštite djece u sajber prostoru i bezbjednog korišćenja interneta.

Imajući u vidu da je CIRT prepoznao malver kao jednu od najvećih prijetnji u crnogorskom sajber prostoru, 4. novembra 2016.godine pokrenut je i pilot projekat u saradnji sa Agencijom za elektronske komukacije i poštansku djelatnost (EKIP) i Internet provajderima u Crnoj Gori.

Projekat je imao za cilj identfikaciju inficiranih računara kao i aktivnosti u cilju oporavka od posledica. Prethodno je urađeno u saradnji sa EKIP i internet provajderima koji posluju u Crnoj Gori. Na ovu temu, u novembru 2016. godine su održani zajednički sastanci i izvršena je testna faza projekta.

Stepen realizacije: Evidentni su pomaci napravljeni na planu snaženja saradnje sa privatnim sektorom. Imajući u vidu važnost postojanja partnerstva javnog i privatnog sektora, isti je prepoznat kao prioritet i kroz Strategiju sajber bezbjednosti Crne Gore 2018-2021.

7. Podizanje nivoa svijesti u društvu i zaštita na Internetu.

U skladu sa zadatkom iz Strategije, Ministarstvo javne uprave je aktivno radilo na edukaciji građana kroz sprovođenje raznih promotivnih kampanja sa posebnim fokusom na zaštitu djece na internetu[9]. Dodatno, Ministarstvo javne uprave je 2017. godine donijelo odluku da se u okviru INFOFESTA-a, svake godine organizuje poseban segment koji se bavi pitanjem sajber bezbjednosti.

[9] https://www.telenor.me/cg/o-telenoru/o-nama/drustvena-odgovornost/odgovorno-poslovanje/surfuj-pametno/
http://www.cirt.me/O_Nama/prijavisadrzaj

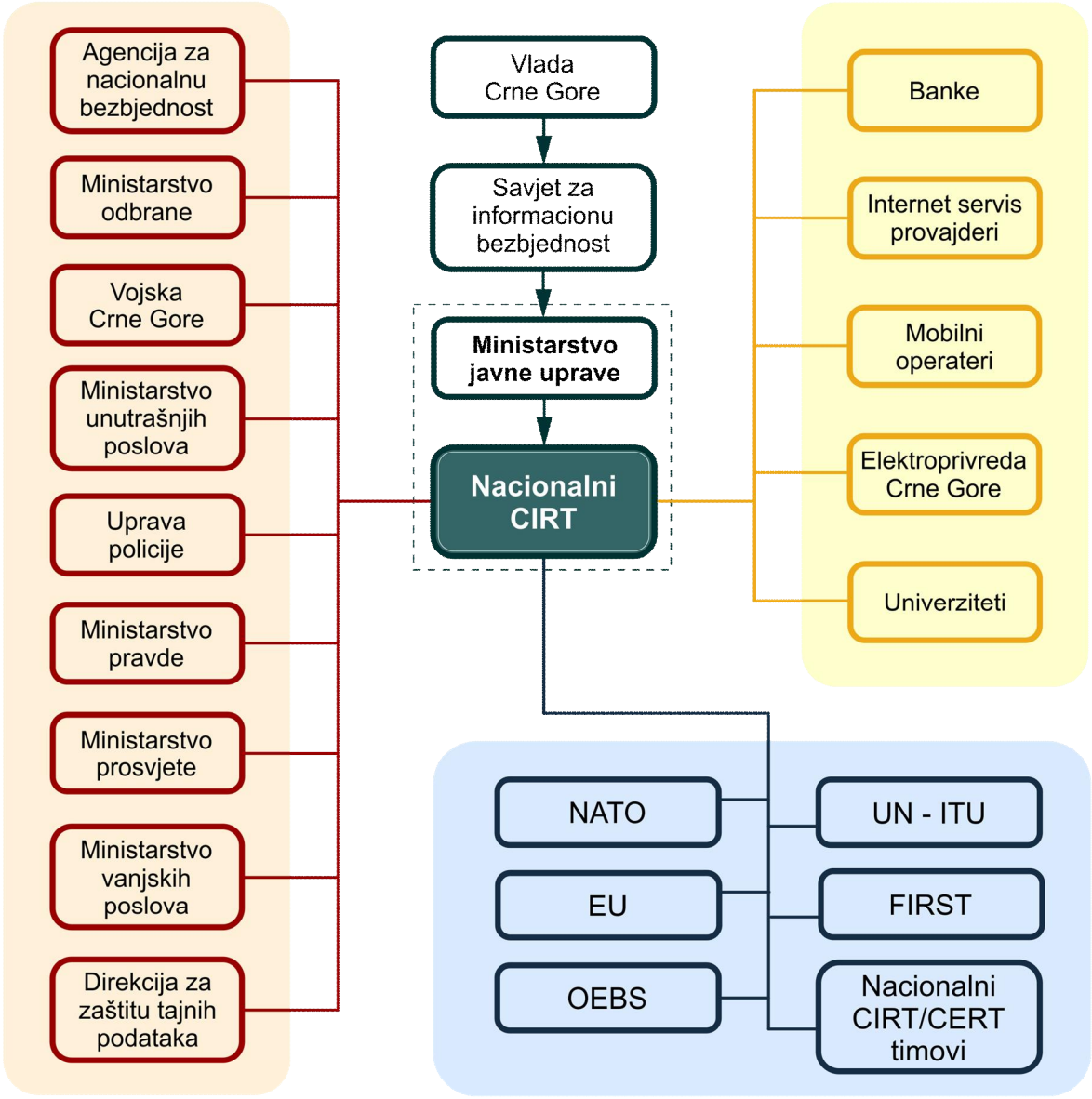
Uprava za kadrove je u svoj redovni program obuka uvrstila i obuku za državne službenike i namještenike na temu sajber bezbjednosti, koja se sprovodi u saradnji sa Ministarstvom javne uprave. Do sada je obuku prošlo 350 državnih službenika i namještenika.

Pored navedenog, sprovođene su usko specijalizovane obuke za službenike koji rade na poslovima sajber bezbjednosti. Neke od najznačajnijih obuka sprovedene su u saradnji sa NATO-om: M6-108 Network Security Course i M6-109 Network Vulnerability Assessment and Risk Mitigation Course, koje je pohađalo po 30 službenika državnih organa.

Stepen realizacije: Ovaj strateški cilj je u značajnoj mjeri realizovan. Međutim, imajući u vidu brzinu razvoja informacionih tehnologija, sve veći broj prijetnji u sajber prostoru, kao i nedostatak usko specijalizovanih kadrova, ovu aktivnost je neophodno sprovoditi u kontinuitetu.

4. Nacionalna organizaciona struktura

4. Nacionalna organizaciona struktura



Grafikon 1: Nacionalna struktura u oblasti sajber bezbjednosti Crne Gore

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

U skladu sa zadatkom da se omogući rano otkrivanje sajber prijetnji i incidenata i adekvatno reaguje i odgovori na iste formirana je 2012. godine Direkcija za zaštitu od računarskih i bezbjednosnih incidenata na internetu – CIRT.

CIRT predstavlja centralno tijelo za koordinaciju prevencije i zaštite od računarskih bezbjednosnih incidenata na internet i drugih rizika bezbjednosti informacionih sistema za područje Crne Gore. CIRT, u skladu sa svojim nadležnostima, djeluje:

•Preventivno – kroz edukaciju, podizanje nivoa svijesti, pružanje korisnih informacija i savjeta u vezi internet sigurnosti i

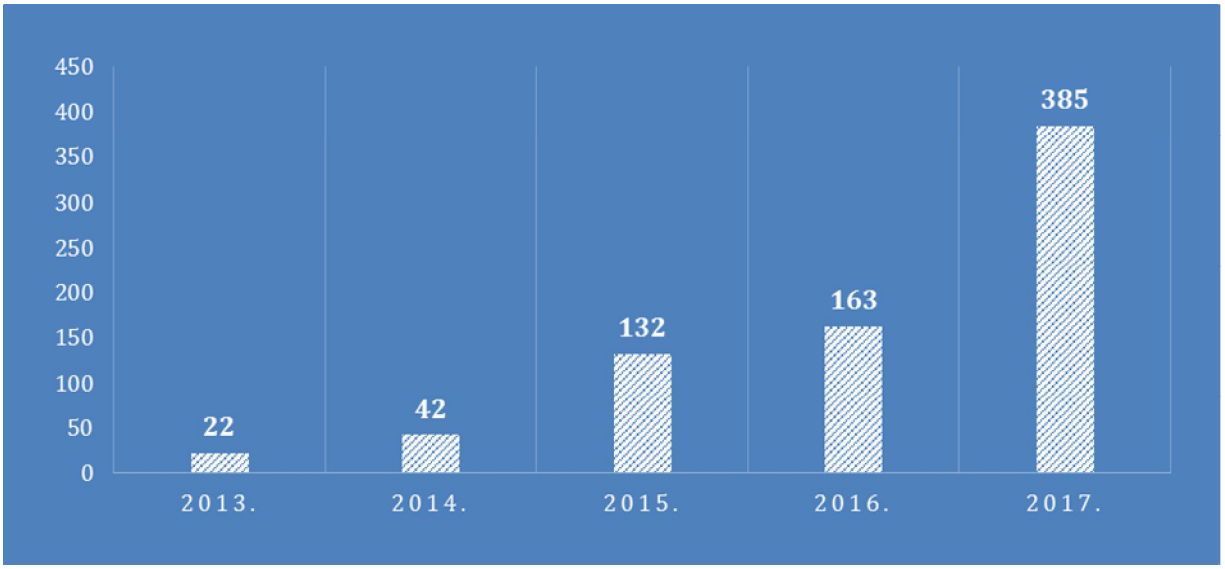
•Reaktivno – kroz analizu i obavljanje detaljnih istraga u slučaju internet incidenata na nacionalnom nivou.

Pored navedenog, CIRT sprovodi aktivnosti na uspostavljanju i unapređenju partnerskih odnosa kako na nacionalnom planu (sa nadležnim resorima, partnerima iz privatnog sektora i akademske zajednice), tako i na međunarodnom planu, a u cilju boljeg i efikasnijeg odgovora na sajber prijetnje.

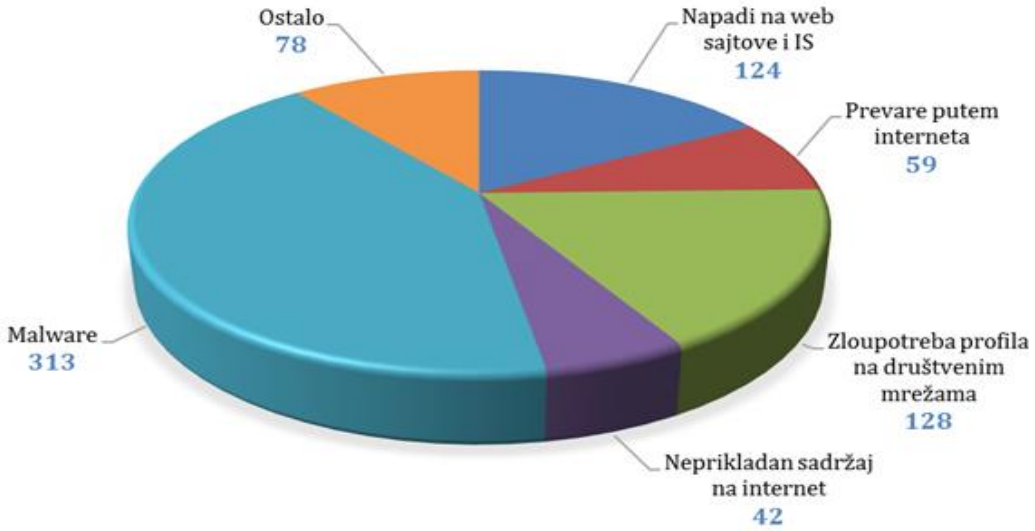
Analizom izvještaja o incidentnim situacijama u Crnoj Gori, koje CIRT izađuje na godišnjem nivou, evidentiran je trend rasta broja prijavljenih incidenata iz godine u godinu, kao i sofisticiranost samih napada.

Godina	Napad na web sajtove i IS	Prevare putem Interneta	Zloupotreba profila na društvenim mrežama	Neprikladan sadržaj na Internetu	Malver	Ostali	UKUPNO
2013	5	3	10	-	1	3	**22**
2014	5	6	20	5		6	**42**
2015	6	17	37	19	17	36	**132**
2016	18	20	36	14	50	25	**163**
2017(do 1. IX)	90	13	25	4	245	8	**385**
UKUPNO	**124**	**59**	**128**	**42**	**313**	**78**	**744**

Tabela 1: Statistika po godinama i tipu napada



Grafikon 2: Prijave po godinama, za periodod 2013. do 1. septembra 2017. godine



Grafikon 3: Statistika prijavljenih incidenata nacionalnom CIRT-u, po tipu, u periodu od 2013. do 1. septembra 2017. godine

U skladu sa Zakonom o izmjenama i dopunama Zakona o informacionoj bezbjednosti (Službeni list Crne Gore, broj 40/2016) 01.08.2017. godine formiran je Savjet za informacionu bezbjednost (Službeni list Crne Gore, broj 48/2017), čime se dobilo krovno tijelo u državi koja će savjetovati Vladu Crne Gore o svim bitnim pitanjima iz ove oblasti.

Zadaci Savjeta su da:

- informiše Vladu Crne Gore o svim bitnim pitanjima koja se tiču sajber bezbjednosti;

- prati sprovođenje Strategije sajber bezbjednosti Crne Gore i akcionih planova za njenu implementaciju;
- prati i koordinira aktivnosti iz oblasti sajber bezbjednosti;
- predlaže mjere za usklađivanje zakonodavnog i administrativnog okvira u cilju unapređenja sajber bezbjednosti Crne Gore;
- radi na unapređenju saradnje u oblasti sajber bezbjednosti između državnih organa i organa uprave i usklađuje njihove aktivnosti;
- radi na unapređenju saradnje sa privatnim sektorom u oblasti sajber bezbjednosti;
- dostavlja Vladi Crne Gore izvještaj o svom radu najmanje jedanput godišnje.

Članovi Savjeta su predstavnici sledećih institucija koje su prepoznate kao **nosioci sajber bezbjednosti** u Crnoj Gori:

- Ministarstvo javne uprave;
- Ministarstvo odbrane;
- Ministarstvo unutrašnjih poslova;
- Ministarstvo pravde;
- Agencija za nacionalnu bezbjednost;
- Direkcija za zaštitu tajnih podataka.

5. Nacionalna sajber odbrana

5. Nacionalna sajber odbrana

Jula 2016. godine Evropska unija usvojila je Direktivu o mrežnoj i informacionoj bezbjednosti (engl. Network Information Security Directive of European Parliament and of the Council 2016/1148). Cilj ove direktive je sveobuhvatno uređenje nacionalne sajber bezbjednosti država članica. Ona se sastoji od pet poglavlja i u cilju ispunjenja obaveza države članice moraju da:

- donesu strategiju sajber bezbjednosti;
- definišu relevantne organe na polju sajber bezbjednosti;
- imaju najmanje jedan tim za odgovor na računarske incidente (engl. CERT – Computer Emergency Response Team). Ovi timovi moraju da pokriju relevantne sektore i servise. Takođe ovi timovi moraju da imaju adekvatne resurse i alate u cilju ispunjenja njihovih kompleksnih funkcija i zadataka;
- urede bezbjednost informacionih sistema vlasnika esencijalnih, kritičnih servisa na tehnički i organizacioni način koji direktiva nalaže;
- urede bezbjednost informacionih sistema vlasnika digitalnih servisa na tehnički i organizacioni način koji direktiva nalaže;
- na dobrovoljnoj osnovi koriste EU standarde koji se preporučuju.

Kolike su razlike među članicama EU po pitanju zaštite mrežne i informacione bezbjednosti može se zaključiti iz same direktive:

„Postojeće sposobnosti nisu dovoljne da osiguraju visok nivo sigurnosti mreže i informacionih sistema u Uniji. Članice imaju veoma različite nivoe pripremljenosti, koje su dovele do podijeljenog pristupa u okviru Unije. Rezultat je nejednak nivo zaštite korisnika i biznisa, i podriva ukupni nivo zaštite mreže i informacionih sistema u okviru Unije.“

„Nacionalna strategija za bezbjednost mreže i informacionih sistema predstavlja radni okvir koji obezbjeđuje strateške ciljeve i prioritete u bezbjednosti mreže i informacionih sistema na nacionalnom nivou.“

U skladu s članom 7 NIS Direktive države članice do 9. maja 2018. godine moraju donijeti nacionalnu strategiju za mrežnu i informacionu bezbjednost, koja se može smatrati jednako vrijednom Nacionalnoj strategiji za sajber bezbjednost, a šest mjeseci nakon toga države moraju završiti identifikaciju operatora ključnih usluga, Komisija je donijela Prilog o djelotvornoj primjeni NIS Direktive COM (2017) 476 od 4.10.2017. godine. Takođe, Komisija je predstavila predlog reforme ENISA-e, koja uključuje njen trajni mandat kao referentne tačke u sajber sistemu EU, te da ona osigura sprovođenje NIS Direktive i predloženog Okvira za sajber sertfikaciju u području informaciono-komunikacionih tehnologija COM (2017) 477 od 4.10.2017. godine. Za pojedine kompanije koje su nosioci kritičnih

sektora vrlo je važna uredba EU – GDPR (General Data Protection Regulation) (EU) 2016/679 od 27.04.2016. godine, koja će biti u primjeni od maja 2018. godine. Kompanije će morati da vode računa o obradi podataka entiteta koji su iz EU, zbog zaprijećene visoke kazne za njeno nepoštovanje, pa moraju početi prilagođavanje svojeg poslovanja novim zahtjevima Uredbe koja se tiču informacionih rizika, bezbjednosti IKT, brze reakcije otkrivanja prijetnji i povrede podataka, oporavka informacija i kontinuiteta uspješnog poslovanja.

Iako NIS direktiva nije obavezujuća za Crnu Goru implementacija njenih preporuka doprinijela bi razvijanju modernog, efikasnog i evropski kompatibilnog nacionalnog koncepta sajber bezbjednosti.

I dok bi se mjesta za diskusiju oko primjene ENISA preporuka moglo naći, kada je u pitanju NATO savez dileme za Crnu Goru kao punopravnog člana nema. NATO je 2016. godine na Samitu u Varšavi proglasio sajber domen za četvrti operacioni domen čime je djelovanje i posledice u okviru sajber prostora izjednačio sa onim u okviru preostala tri domena: voda, vazduh i zemlja. Dodatno, jula 2016. godine šefovi i predsjednici vlada država članica NATO alijanse obavezali su se da će sajber prostor tretirati isto u strateškom pogledu kao i preostala tri operativna domena u tzv. „sajber obećanju“ (*eng. „cyber pledge“*). Između ostalog, zemlje članice su se obavezale na:

- jačanje i povećanje kapaciteta odbrane nacionalnih mreža i infrastruktura i to smatrati prioritetom;
- raspoređivanje adekvatnih resursa na nacionalnom nivou kako bi se ojačali kapaciteti za sajber odbranu;
- jačanje saradnje između relevantnih nacionalnih organa sajber odbrane u cilju efikasnije saradnje i razmjene najboljih praksi
- razvijanje vještina i svijesti među svim akterima sajber odbrane na nacionalnom nivou od bazične sajber higijene do najsofisticiranije i robusne sajber odbrane;
- podsticanje programa edukacija, obuka i vežbi na polju sajbera, i poboljšanje obrazovnih institucija u cilju izgradnje povjerenje i znanja u okviru Alijanse.

Razvoj nacionalnog koncepta za sajber bezbjednost bi danas trebalo usmjeravati kroz dva novonastala bitna faktora od usvajanja i implementacije prve nacionalne strategije za sajber bezbjednost – pristupanje NATO savezu i otvaranje pregovaračkog poglavlja 11 Informatičko društvo.

Vlada Crne Gore će nastaviti da preduzima aktivnosti u pravcu realizacije Strategijom prepoznatih strateških ciljeva na način da obezbijedi dalje unapređenje koncepta sajber bezbjednosti Crne Gore koji će biti

kompatibilan sa konceptima najrazvijenijih zamalja članica EU i NATO saveza.

Posebna pažnja biće posvećena usaglašavanju u pogledu standardizacije pojmova, metoda, polisa i procedura u skladu sa prihvaćenim evropskim i međunarodnim standardima.

5.1. Kapaciteti za sajber odbranu

Na osnovu Globalnog sajber bezbjednosnog indeksa[10] izrađenog 2017. godine od strane Međunarodne telekomunikacione unije Crna Gora zauzma 71. mjesto u oblasti sajber bezbjednosti sa koeficijentom 0,422, od ukupno 193 države koje su obuhvaćene ovim istraživanjem. U odnosu na region Crna Gora se nalazi ispred Albanije (89), Srbije (90), Bosne i Hercegovine (136) i Slovenije (84), dok su Hrvatska (41) i Makedonija (55) bolje rangirane.

STRATEŠKI CILJ:
Vlada Crne Gore će nastaviti sa posvećenim radom na daljem jačanju sajber bezbjednosnih kapaciteta u smislu obezbjeđivanja adekvatnih ljudskih, finansijskih resursa kao i drugih potreba neophodnih za efikasne i agilne sajber kapacitete institucija Crne Gore koje imaju za cilj da obezbijede siguran sajber prostor, omoguće podsticaj biznisa i u krajnjem doprinesu ekonomskom prosperitetu Crne Gore.

PRAVCI DJELOVANJA I INDIKATORI:

a. Relevantne institucije na polju sajber bezbjednosti će osnovati CIRT timove ili prepoznati službenike čija će osnovna funkcija biti aktivnosti iz domena sajber bezbjednosti tzv. **lokalni CIRT**. **Indikator** uspjeha će biti procentualno povećanje trenutnog broja CIRT timova u odnosu na broj uspostavljenih i broj institucija koje trebaju da imaju CIRT timove.

b. Relevantne institucije moraju imati kapacitete da prepoznaju, identifikuju i urade godišnje ili ukoliko je potrebno vremenski kraće analize rizika po informacione sisteme u okviru istih ili u okviru njihove nadležnosti. **Indikator** uspjeha predstavljaće broj izrađenih analiza rizika u odnosu na broj institucija.

c. Posebni organi ili organizacione jedinice, u okviru institucija koje su prepoznate kao nosioci funkcije sajber bezbjednosti Crne Gore, moraju da imaju opredijeljena budžetska sredstva svake godine, kojima bi nabavljali adekvatne resurse i alate za efikasno funkcionisanje. **Indikatori** uspjeha će predstavljati broj institucija koje imaju budžetska sredstva opredijeljena za sajber bezbjednost i broj institucija koje imaju trend povećanja godišnjeg budžeta za navedene potrebe.

d. Relevantni organi moraju definisati optimalan broj zaposlenih službenika u njihovom CIRT timu odnosno službenika zaduženih za sajber bezbjednost u cilju adekvatnog odgovora na prijetnje, izazove, analize rizika i potencijalne napade na njihove informacione sisteme. Prethodno mora

[10] Globalni sajber bezbjednosni indeks za 2017. Link: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

biti urađeno na godišnjem nivou a kako bi imali pregled broja zaposlenih i broja potrebnih službenika na Nacionalnom nivou. Na osnovu preporuka ENISE[11] minimalan broj zaposlenih u CIRT koji ima funkciju 24/7 jeste 12. **Indikator** uspjeha predstavlja izvještaj o minimalnom broju službenika za sajber bezbjednost.

5.2. Centralizacija sajber ekspertize i resursa

STRATEŠKI CILJ:
Vlada Crne Gore će preduzimati aktivnosti na centralizaciji i okupljanju ekspertize u oblasti sajber bezbjednosti kako bi se: ojačali kapaciteti za adekvatan odgovor na sofisticirane sajber prijetnje po kritične infomatičke infrastrukture i druge bitne informacione sisteme; razumijeli rizici po sajber prostor Crne Gore; pružile adekvatne preporuke i unaprijedila saradnja sa privatnim i javnim sektorom.

U vodećim državama na planu sajber kapaciteta i odbrane pristupilo se osnivanju samostalnih institucija za sajber bezbjednost i odgovor na incidentne situacije, što se pokazalo kao neophodni i veoma efikasni korak. Tako je u Ujedinjenom Kraljevstvu Velike Britanije i Sjeverne Irske 2015. godine osnovan Centar za sajber bezbjednost koji je okupio nekoliko institucija između kojih i državni tim za odgovor na sajber incidente (CIRT tim). U Republici Hrvatskoj je 2012. godine formiran Zavod za sigurnost informacionih sistema (ZSIS) koji je takođe obuhvatio funkciju Nacionalnog CIRT-a, dok je u Australiji osim Centra za sajber bezbjednost, koji predstavlja glavnu instituciju ekspertize i autoriteta, operativan i Zajednički centar za sajber prijetnje koji osim državnog okuplja privatni sektor i akademsku zajednicu, i predstavlja inovativan i efikasan pristup sajber bezbjednosti u smislu bolje razmjene informacija i povjerenja između različitih aktera, jačanja saradnje i udruživanja snaga, a sve u cilju jedinstvenog odgovora na kompleksne sajber prijetnje, napade i izazove.

PRAVCI DJELOVANJA I INDIKATORI:

a. U skladu sa Strategijom razvoja informacionog društva[12] do 2020. godine Nacionalni CIRT tim će do 2018. godine imati 10 službenika, a do 2020. godine imati 20 službenika. **Indikator** uspjeha predstavljaće ispunjenost zadatih rokova i broj zaposlenih u Nacionalnom CIRT-u.

b. U okviru Nacionalnog CIRT-a sistematizovaće se dva odeljenja - za odgovor na incidente, tehničkog karaktera i za strateške pravce, politike i preventivu. **Indikator** uspjeha predstavljaće izmjena Pravilnika o unutrašnjoj organizaciji i sistematizaciji Ministarstva javne uprave.

c. Za funkcionisanje Nacionalnog CIRT-a opredijeliće se dvije specijalizovane

[11] Više na linku: https://www.enisa.europa.eu/publications/csirt-setting-up-guide

[12] http://www.gov.me/sjednice_vlade/166

prostorije u kojima će se obezbijediti rad i eksperata iz drugih institucija u slučaju napada na KII i napada širokih razmjera na Crnu Goru. **Indikator** uspjeha broj prostorija koje ispunjavaju minumum tehničkih karakteristika u odnosu na broj predviđenih

d. Nacionalni CIRT će u redovnim vremeskim intervalima organizovati specijalističke vježbe, simulacije napada na KII i napada širokih razmjera za pripadnike relevantnih organa, kao i kompanije nosioce KII. **Indikator** uspjeha predstavljaće broj organizovanih vježbi i uključenih aktera.

5.3 Zaštita kritične informatičke infrastrukture

	KRITIČNI SEKTORI	**NOSIOCI KRITIČNOG SEKTORA**
1	Informacione i komunikacione tehnologije	Ministarstvo javne uprave
2	Bankarstvo i finansije	Ministarstvo finansija
3	Energetika	Ministarstvo ekonomije
4	Zdravstvo	Ministarstvo zdravlja
5	Poljoprivreda, bezbijednost hrane, šumarstvo i vodoprivreda	Ministarstvo poljoprivrede i ruralnog razvoja
6	Nacionalna odbrana i bezbjednost	Ministarstvo odbrane / Ministarstvo unutrašnjih poslova / Ministarstvo pravde/ Agencija za nacionalnu bezbjednost
7	Transport	Ministarstvo saobraćaja i pomorstva
8	Državni organi/Usluge Vlade CG	Ministarstvo javne uprave

Tabelarni prikaz kritičnih sektora i nadležnih institucija

Na osnovu Strategije sajber bezbjednosti 2013-2017 donijete su **Izmjene i dopune Zakona o informacionoj bezbjednosti** ("Službeni list Crne Gore, broj 40/2016") kojim je i formalno-pravno (prethodno KII je definisana kroz Metodologiju za izbor KII) definisana Kritična informatička infrastruktura kao: „***informacioni sistemi organa čijim bi se prekidom rada ili uništenjem ugrozili život, zdravlje, bezbjednost građana i funkcionisanje države i od čijeg funkcionisanja zavisi vršenje djelatnosti od javnog interesa***“.

U okviru **prve faze** izrađena je detaljna analiza informacionih sistema nadležnih organa.

U okviru **druge faze** izvršena je detaljna analiza informacionih sistema državnih organa.

U okviru **treće faze** proslijeđen je upitnik privatnom sektoru na osnovu kojeg je dobijena analiza njihovih informacionih sistema, čime je kompletirana analiza informacionih sistema svih definisanih kritičnih sektora.

Na osnovu pomenute analize, a zatim i analize kritičnosti donijet je predlog liste kritičnih informacionih sistema, nakon čega je Vlada Crne Gore zadužila Ministarstvo javne uprave da usvoji konačnu listu KII, a zatim definiše mjere zaštite.

U Evropskoj uniji prepoznate su dvije glavne metode zaštite KII: prva gdje čitavim procesom upravlja država, koju je primijenila i Crna Gora, i druga gdje glavnu funkciju imaju operatori/vlasnici KII.

U Crnoj Gori prepoznato je osam kritičnih sektora u okviru kojih se nalazi jedna ili više KII. Kontrola bezbjednosti KII u okviru sektora pripada resornim ministarstvima ili drugim državnim organima koji imaju zakonsku osnovu i obavezu za bezbjednost i regulaciju tih sektora. Krovno tijelo za koordinaciju aktivnosti, razvijanje saradnje i drugih djelatnosti vezanih za ovu oblast jeste Nacionalni CIRT.

Studija slučaja

U februaru 2017. godine niz servisa državnih organa bio je pod intezivnim i kontinuiranim DDoS napadom koji je trajao dvije nedelje.

Analizom je utvrđeno da je napad dolazio sa širokog spektra IP adresa rasprostranjenih širom svijeta i predstavlja mrežu tzv. zombi, inficiranih računara, karakterističnih za ovu vrstu napada, u okviru ovog perioda nekoliko državnih servisa je bilo pod kontinuiranim sajber napadom.

Predmetni incident je doprinio daljem širenju svijesti o tome kakve posledice može da izazove napad u sajber prostoru. Istovremeno državni organi koji se bave odbranom imali su priliku da testiraju svoje kapacitete i razviju bližu i efikasniju saradnju sa partnerima iz privatnog sektora u cilju efikasnije odbrane od ovog tipa napada.

STRATEŠKI CILJ:

Vlada Crne Gore će nastaviti da jača kapacite za odbranu KII, a s obzirom da noseću ulogu na ovom polju ima nacionalni CIRT - on mora imati adekvatne resurse i alate kako bi na efikasan način mogao da razumije, analizira i odgovori na širok spektar prijetnji na ovom polju.

Resursi državnih organa zaduženih za kontrolu bezbjednosti KII moraju biti adekvatni zadatku, odnosno državni organi moraju imati službenike koji razumiju prijetnje i rizike koji postoje za specifične KII koje pripadaju njihovom sektoru. Ljudski i tehnički resursi moraju biti ojačani u cilju efektivnog obavljanja ove funkcije.

U cilju efikasne odbrane neophodno je i identifikovanje i suštinsko razumijevanje rizika koji se odnose na KII, odnosno na oblasti djelovanja, različite informatičke platforme, sisteme, funkcije i tehnologije od kojih se sajstoji KII, što predstavlja kompleksan zadatak i izazov. S obzirom da veliki dio KII pripada privatnom sektoru Vlada Crne Gore će pružati podršku prilikom identifikovanja rizika

po kritične sisteme i gdje je neophodno utvrditi dodatne mjere zaštite u cilju zaštite nacionalnih interesa.

Vlada Crne Gore će takođe nastaviti da unapređuje zakonodavni okvir, standarde i obaveze koje vlasnici KII moraju da ispune, što je na liniji harmonizacije sa Direktivom Evropke unije o mrežnoj i informacionoj bezbjednosti.

***PRAVCI DJELOVANJA* I INDIKATORI:**

a. Vlasnici identifikovanih KII dužni su da rade godišnje analize rizika. Nacionalni CIRT tim u saradnji sa ostalim nadležnim CIRT timovima, ima funkciju da uradi reviziju analiza, da pruži pomoć u izradi analiza gdje vlasnici KII nemaju dovoljnih kapaciteta. **Indikator** uspjeha predstavljaće broj urađenih analiza u odnosu na broj KII, kao i kvalitet istih.

b. Donošenje podzakonskih akata za zaštitu KII. Ova regulativa treba da definiše procedure komunikacije između vlasnika KII i nadležnih istitucija, kao i osnovne tehničke i organizacione mjere koje vlasnici KII moraju da ispune. **Indikator** uspjeha predstavljaće usvojena Uredba o mjerama zaštite KII.

c. Nacionalni CIRT tim u saradnji sa ostalim CIRT timovima treba da uspostavi i formalizuje strateška partnerstva sa vlasnicima KII, gdje između ostalog treba specificirati razmjenu informacija, načine razmjene informacija i ekspertize. **Indikator** uspjeha predstavljaće broj formalizovanih partnerstava sa nosiocima KII.

5.4 Međuinstitucionalna saradnja

STRATEŠKI CILJ:

Prepoznata je potreba za jačanjem međuinstitucionalne saradnje, pri čemu će poseban akcenat biti stavljen na efikasnu i pravovremenu razmjenu informacija i najboljih praksi. U tom kontekstu, nadležne institucije će raditi na snaženju komunikacionih metoda, kroz, između ostalog organizovanju vježbi kriznog komuniciranja u slučaju sajber incidenata i napada većih razmjera. Vježbe će imati za cilj definisanje jasnih procedura komuniciranja u kriznim situacijama, kao i pravovremeno revidiranje istih.

PRAVCI DJELOVANJA I INDIKATORI:

a. Kako bi saradnja i komunikacija među institucijama bila dodatno olakšana, evidentirana je potrebna imenovanja kontakt osoba za sajber bezbjednost ispred svih uključenih aktera. **Indikator** uspjeha predstavljaće broj imenovanih kontakt osoba u odnosu na broj institucija.

b. Uspostavljanje javno dostupnog registra sajber eksperata koji bi vodilo nadležno Ministarstvo za ovu oblast. **Indikator** uspjeha predstavljaće funkcionisanje registra sajber eksperata.

c. Razvoj platforme za dijalog i razmjenu informacija koja bi povezala eksperte za sajber bezbjednost iz javnog i privatnog sektora kako na lokalnom, tako i na nacionalnom nivou. **Indikator** uspjeha predstavljaće operativna platforma.

d. Uspostavljanje inter-resorne radne grupe na tehničkom nivou koja bi okupila eksperte sajber bezbjednosti i stvorila kapacitete za odbranu od sajber napada. **Indikator** uspjeha predstavljaće formirana inter-resorna grupa.

e. U cilju efikasnosti, koordinacije i komunikacije inter-resorna radna grupa organizovaće simulacije i vježbe. **Indikator** uspjeha predstavljaće broj organizovanih vježbi na godišnjem nivou, dužina trajanja vježbi, kao i broj uključenih institucija.

f. Izrada pravilnika i procedura za razmjenu informacija o sajber incidentima, načinima komuniciranja u slučaju sajber napada, načinima pomoći i kooperaciji između državnih organa. **Indikator** uspjeha predstavljaće definisan pravilnik i procedure razmjene informacija o sajber incidentima i komuniciranja između organa.

5.5. Zaštita podataka

STRATEŠKI CILJ:

Vlada Crne Gora će u cilju sprovođenja adekvatne zaštite važnog dijela informatičke infrastrukture jačati nacionalne kapacitete potrebne za sprovođenje bezbjednosne akreditacije komunikaciono-informacionih sistema i procesa u kojima se koriste tajni podaci, kao i kapaciteti u oblasti kripto zaštite.

Zakonom o tajnosti podataka prepoznat je princip označavanja podataka određenim stepenom tajnosti i način ophođenja prema tim podacima, od onih označenih najnižim stepenom tajnosti čijim bi otkrivanjem nastupile štetne posljedice za ostvarivanje funkcije organa, do podataka najvećeg stepena tajnosti čije otkrivanje bi ugrozilo ili nanijelo neotklonjive štetne posljedice za bezbjednost i interese Crne Gore. Informatizacija poslovnih procesa učinila je da se ovi podaci kreiraju, obrađuju i čuvaju u elektronskoj formi i zbog potrebe za efikasnom razmjenom podataka sve više prenose kroz sajber prostor. Da bi se obezbijedila adekvatna zaštita i podigao nivo kulture postupanja sa tajnim i osjetljivim podacima u elektronskoj formi, potrebno je jačati nacionalne kapacitete potrebne za sprovođenje zakonski propisane bezbjednosne akreditacije komunikaciono-informacionih sistema i procesa u kojima se koriste tajni podaci stepena tajnosti POVJERLJIVO i TAJNO i obezbijediti adekvatan sistem menadžmenta bezbjednošću informacija u sistemima u kojima se koriste podaci stepena tajnosti INTERNO[13], kao i u sistemima u kojima se rukuje neklasifikovanim osjetljivim podacima. Takođe, potrebno je dugoročno planirati nacionalne kapacitete u cilju razvoja domaćih kriptografskih rješenja.

PRAVCI DJELOVANJA I INDIKATORI:

a. U martu 2017. godine donešen je set pravnih propisa neophodnih za sprovođenje sertifikacije komunikaciono informacionih sistema i procesa u kojima se koriste tajni podaci većih stepena tajnosti. Prepoznato je da postoji prostor za unapređenje ovog seta propisa, posebno u dijelu sertifikacije '*standalone*' mašina i interkonekcije komunikaciono-informacionih sistema. **Indikator uspjeha** predstavljaće izrada odgovarajućih pravnih akata i pratećih dokumenata od strane međuresorne radne grupe.

b. Jačanje informatičkih kapaciteta državnog organa nadležnog za sprovođenje bezbjednosne akreditacije komunikaciono-informacionih sistema i procesa u kojima se koriste tajni podaci (SAA – engl. *Security Accreditation Authority*) i nadležnog za upravljanje materijalima za kriptografsku zaštitu tajnih podataka (NDA – engl. *National Distribution Authority*). **Indikator uspjeha** je broj novozaposlenih informatičara u Direkciji za zaštitu tajnih podataka koji će se baviti akreditacijom

[13] Zakon o tajnosti podataka ("Sl. list Crne Gore", br. 14/13 od 15.03.2013) i Uredba o bližim uslovima i načinu sprovođenja informatičkih mjera zaštite tajnih podataka, ("Sl. list Crne Gore", br. 57/10 od 01.10.2010)

komunikaciono-informacionih sistema i upravljanjem kripto materijalima.

c. Jačanje institucionalnih kapaciteta potrebnih za sprovođenje sertifikacije komunikaciono-informacionih sistema i njihovih interkonekcija kroz uvođenje sistematizovane funkcije koja obuhvata opisa posla za informacionu bezbjednost tajnih podataka u državnim institucijama u kojima se u većoj mjeri rukuje tajnim podacima u elektronskoj formi (za veće stepene tajnosti sistematizovano kao posebno radno mjesto, za najniži stepen tajnosti moguće kao dodati opis poslova kod postojećeg radnog mjesta). **Indikator uspjeha** je broj sistematizovanih radnih mjesta sa opisom poslova vezanihza informacionu bezbjednost tajnih podataka.

d. Sertifikacija komunikaciono-informacionih sistema u kojima se koriste podaci većih stepena tajnosti, uvođenje sistema menadžmenta bezbjednošću informacija i upravljanja rizika u komunikaciono-informacionim sistemima u kojima se koriste tajni podaci stepena tajnosti INTERNO (ISO/IEC 27000 certifikacija uz dodatne mjere bezbjednosti) i neklasifikovani osjetljivi podaci (ISO/IEC 27001). **Indikator uspjeha** je broj sertifikovanih komunikaciono-informacionih sistema i sprovedenih internih revizija u cilju provjere implementacije standarda.

e. Uspostavljanje saradnje sa obrazovnim i naučnim institucijama u cilju dugoročne edukacije i osposobljavanja kadra za potrebe kreiranja nacionalnih kriptografskih rješenja. **Indikator uspjeha** je broj uspostavljenih saradnji i iz njih pokrenutih obrazovnih ili naučnih projekata.

5.6. Edukacija u oblasti sajber bezbjednosti

STRATEŠKI CILJ:

adležni državni organi u cilju najbolje sajber bezbjednosne prakse će informisati o najnovijim sajber prijetnjama i preduzimati aktivnosti na edukaciji građana i organizacija u pogledu mehanizmima zaštite u sajber prostoru. Potrebni su održivi, kontinuirani i koordinirani napori kako bi se postigle šire promjene ponašanja i kako bi osigurali da sve ciljne grupe javni i privatni sektor, kao i pojedinačni građanin, razumiju rizike i prijetnje koje postoje u sajber prostoru.

Širenje svijesti o prijetnjama u sajber prostoru, kao i njihovom uticaju na cjelokupno društvo postalo je vitalno. Kroz podizanje svijesti, individualni i korporativni korisnici mogu naučiti kako da se ponašaju i osjećaju sigurnijim i spremnim da posluju u online svijetu.

Edukacija službenika i građana kroz objavljivanje raznih sigurnosnih savjeta, uputstava i upozorenja bazira se na aktuelnim trendovima u tehnologiji i distribuciji relevantnih znanja regionalnih i međunarodnih stručnjaka. Važan segment u širenju svijesti je i unapređenje sadržaja na portalu sa materijalima, koji se kontinuirano ažuriraju u skladu sa novim tehnologijama, vezanim za sigurnost informacija (smjernice, priručnik, prezentacije, vebinari, predavanja).

Fokus na različite ciljne grupe je rezultat uspješnih i efikasnih kampanja o širenju svijesti o bezbjednosnim izazovima. Kontinuirano praćenje i evaluacija kampanje je korisna u smislu identifikacije novih nastalih potreba i prilagođavanja procesa kampanje. Održivi ljudski i finansijski resursi i kontinuirani monitoring mogu doprinijeti povećanju fleksibilnosti i prilagodljivosti kampanje.

PRAVCI DJELOVANJA I INDIKATORI:

a. U cilju promovisanja i širenja kulture o sajber bezbjednosti neophodno je kontinuirano nastaviti sa učešćem na i organizovanjem konferencija, radionica, obuka, kao i sa izradom publikacija, pisanjem radova i članaka, te i, gostovanjima u obrazovnim emisijama. **Indikator** uspjeha predstavljaće broj održanih konferencija/radionica/obuka i gostovanja u obrazovnim emisijama.

b. Kako je konstantna edukacija, praćenje trendova i širenje svijesti od velikog značaja za sajber bezbjednost, trebalo bi konstantno unapređivati sadržaj na portalu CIRT.ME, sa materijalima vezanim za bezbjednost, koji se kontinuirano ažuriraju u skladu sa novim tehnologijama (savjeti, upozorenja, obavještenja, smjernice, priručnici, prezentacije, vebinari, predavanja). **Indikator** uspjeha predstavljaće, uz broj objavljenih sadržaja na portalu CIRT.ME i broj ažuriranih materijala.

c. Potrebno je edukovati nastavni kadar kako bi se svjest o sajber bezbjednost kod njih podigla na veći nivo jer najviše

vremena provode u neposrednom radu sa djecom pa su u prilici da utiču i na podizanju njihove svijesti o ovoj temi. **Indikator uspjeha** predstavljaće broj obučenih nastavnika po predhodno utvrđenom programu obuke.

d. Posebna ciljna grupa koja je prepoznata su školski pedagozi i psiholozi. Većina problema najčešće se riješava u pedagoško-psihološkoj službi škole pa je njihovo poznavanje i razumjevanje ove problematike od velikog značaja za pomoć djeci. Predhodno je potrebno utvrditi da li su svi školski pedagozi digitalno pismeni i ukoliko nisu neophodno im je pružiti elementarno znanje rada na računaru a nakon toga sprovesti obuke koje se odnose na sajber bezbjednost. **Indikator uspjeha** je broj obučenih pedagoga i pihologa na osnovu unaprijed definisanog programa obuke.

e. Redavan predmet Informatika sa tehnikom koji se izučava tek od petog razreda osnovne škole a obuhvata određeni broj nastavnih jedinica nije dovoljan kada je tema sajber bezbjednost u pitanju pa je za djecu školskog uzrasta neophodno organizovanje niza vannastavnih aktivnosti na ovu temu, posebno za djecu manjeg uzrasta. **Indikator uspjeha** broj održanih radionica, takmičenja, debati itd, kao i broj djece koji je obuhvaćen aktivnostima.

f. Neophodno je razviti niz materijala na razne teme sajber bezbjednosti koje će biti prilagođene različitim uzrastima djece. Materijale objaviti na školskom portalu (www.skolskiportal.edu.me) u kategoriji Bezbjednost djece na internetu. **Indikator uspjeha** bi bio broj kreiranih materijala (foto, video, prirucnik, smjernica, preporuka, igrica itd).

5.7. Partnerstvo javnog i privatnog sektora

STRATEŠKI CILJ: Vlada Crne Gore će i u narednom periodu nastaviti sa posvećenim radom u cilju podrške, kako u odgovoru na incidente, tako i u dijeljenju informacija i zajedničke inicijative u parnerstvu sa privatnim sektorom. Dakle, jedino visok stepen komunikacije, saradnje i integracije može biti efikasan način da se razumije i na pravi način odgovori na potrebe i izazove privatnih kompanija, a u cilju da se preduzmu neophodne mjere kako bi se postigao dovoljan stepen bezbjednosti.

Poboljšanje sajber bezbjednosti zahtijeva kombinovani, višekorisnički, sveobuhvatni pristup koji se fokusira na saradnju sa privatnim preduzećima. Saradnja omogućava da se kroz zajedničko istraživanje i razmjenu iskustava i prakse obezbijedi da nijedan dio kritične infrastrukture, bilo u javnim ili privatnim rukama, ne postane slaba veza i ranjivost.

Partnerstvo javnog i privatnog sektora predstavlja efikasan alat u zaštiti nacionalnih interesa. Podjela informacija, stručnosti i znanja je oblik strateškog partnerstva među zainteresovanim stranama iz javnog i privatnog sektora. U skladu sa Zakonom o izmjenama i dopunama Zakona o informacionoj bezbjednosti je formiran Savjet za informacionu bezbjednost koji predstavlja okvir za stalnu razmjenu informacija između javne uprave, predstavnika privrede, nauke i istraživanja. Preko Savjeta za informacionu bezbjednost bi trebalo obezbijediti procedure za razmjenu informacija između državnih organa i ključnih institucija iz privatnog sektora, naročito internet provajderom, bankarskim sektorom,Elektroprivredom. Izgradnja uspješnog partnerstva javnog i privatnog sektora uzima u obzir različite elemente kao i izazove i barijere sa kojima se mogu suočiti takve strukture. Uspostavljanje efikasne saradnje između zainteresovanih strana predstavlja jedan od glavnih izazova zbog različitih interesa, povjerenja, kompetencije i nedostatka jasne upravljačke strukture. Kompanije nerado prijavljuju bezbjednosne incidente zbog potencijalnog gubitka reputacije pa je uspostavljanje povjerenja proces koji zahtijeva obiman dijalog, kao i vrijeme i trud. Partnerstva zahtijevaju jasan okvir koji određuje uloge javnog i privatnog sektora, njihove odnose i područja za saradnju.

PRAVCI DJELOVANJA I INDIKATORI:

a. U cilju razvoja efikasnog odgovora za sajber bezbjednost trebalo bi raditi na unaprjeđenju i institucionalizaciji saradnje između javnog i privatnog sektora. **Indikator uspjeha** predstavljaće broj uspostavljenih javno-privatnih partnerstava.

b. Izrada procedura za razmjenu informacija o sajber incidentima, načinima komuniciranja u slučaju sajber napada, načinima pomoći i kooperaciji između javnog i privatnog sektora. **Indikator uspjeha** predstavljaće definisan pravilnik za proceduru razmjene informacija o sajber incidentima i komuniciranja između javnog i privatnog sektora.

5.8. Regionalna i međunarodna saradnja

STRATEŠKI CILJ:

Vlada Crne Gore će nastaviti sa regionalnim i međunarodnim aktivnostima i vršiti svoj uticaj ulaganjem u partnerstva koja oblikuju globalnu evoluciju sajber prostora na način koji unapređuje i širi ekonomske i bezbjednosne interese i poboljšava kolektivnu bezbjednost.

S obzirom na globalnu prirodu Interneta, a time i na probleme sajber bezbjednosti, saradnja na regionalnom i međunarodnom planu je neophodna u obezbeđivanju sajber prostora Crne Gore.

Zbog sve većeg obima bezbjednosnih incidenata, postojeće mogućnosti tima za odgovor na incidente (CIRT-a) više nisu dovoljne. Kako bi se omogućio odgovarajući odgovor i zaštitili nacionalni interesi treba nastaviti sa saradnjom i aktivnostima sa regionalnim i međunarodnim partnerima.

Neophodno je dodatno osnažiti odnose sa partnerima na bilateralnom i multilateralnom nivou, uključujući EU, NATO, OEBS i UN, posebno kroz kolektivnu odbranu i kooperativnu sigurnost.

Takva saradnja olakšava dobru razmjenu iskustava, znanja i najboljih praksi, a sve to doprinosi jačanju nacionalne sigurnosti. Stoga, Crna Gora će nastaviti da promoviše učešće svojih predstavnika u međunarodnim organizacijama, kao i u profesionalnim vježbama i udruženjima u ovoj oblasti.

PRAVCI DJELOVANJA I INDIKATORI:

a. Kako razmjena regionalnih i međunarodnih iskustava i najbolje prakse doprinosi jačanju i razvoju sajber bezbjednosti treba nastaviti sa aktivnim učešćem kroz zajedničke vježbe, obuke, sastanke, forume, konferencije, seminare. **Indikator uspjeha predstavljaće** broj održanih obuka, konferencija, seminara, vježbi, sastanaka i biće kvalitativnog karaktera.

b. U cilju jačanja saradnje sa ključnim međunarodnim institucijama u oblasti sajber bezbjednosti treba nastaviti sa kontinuiranom saradnjom sa organizacijama čiji smo član (FIRST, ITU, NATO) i raditi na pristupanju i promociji novih partnerstava. **Indikator uspjeha** predstavljaće broj sklopljenih partnerstava, potpisanih ugovora i memoranduma.

6. Monitoring

6. Monitoring

Da bi se obezbjedila adekvatna implementacija Strategije sajber bezbjednosti Crne Gore 2018-2021 i pratećih akcionih planova, na osnovu člana 13a stav 1 Zakona o informacionoj bezbjednosti (''Službeni list CG'', br. 14/10 i 40/16), Vlada Crne Gore donijela je Odluku o obrazovanju Savjeta za informacionu bezbjednost sa zadatkom, između ostalih, da prati sprovođenje Strategije i akcionih planova.

Organi koji su prepoznati kao nosioci aktivnosti definisanih Strategijom i pratećim akcionim planovima dužni su da Savjetu za informacionu bezbjednost dostavljaju kvartalne izvještaje o realizaciji istih.

Na osnovu dostavljenih izvještaja Savjet će analizirati ostvarene rezultate i u skladu sa svojim nadležnostima dati mišljenje i preporuke ukoliko stepen realizacije ne prati utvrđenu dinamiku.

Godišnje, Savjet će Vladi Crne Gore podnositi izvještaj o radu, koji će tretirati stepen ispunjenosti strateških ciljeva definisanih Strategijom i aktivnosti iz Akcionog plana, kao i sadržati predlog mjera za dalje unapređenje sajber bezbjednosti Crne Gore.

7. Zaključna razmatranja

7. Zaključna razmatranja

Funkcionisanje svakog pojedinca u modernom dobu se ne može zamisliti bez upotrebe informaciono-komunikacionih tehnologija. Razvoj tehnologija podstiče ekonomski i socijalni razvoj jedne države i omogućava konkurentnost i njeno pozicioniranje u regionu i Evropi. Samim tim, Crna Gora ne može i ne smije biti izuzetak.

Uzimajući u obzir prethodno navedeno i činjenicu da je broj prijetnji u sajber prostoru u stalnom porastu, paralelno sa daljim razvojem informacionog društva neophodno je konstantno raditi na unaprjeđenju sajber bezbjednosti.

Vlada Crne Gore je posvećena rastu i prosperitetu kroz snažnu sajber bezbjednost.

U proteklom periodu, na osnovu člana 13a Zakona o informacionoj bezbjednosti („Sl. list CG“, br. 14/10 i 40/16), Vlada Crne Gore je donijela Odluku o obrazovanju Savjeta za informacionu bezbjednost. Savjet će, između ostalog, pratiti sprovođenje Strategije sajber bezbjednosti, kroz dostavljanje kvartalnih izvještaja od strane organa koji su prepoznati kao nosioci aktivnosti definisanih Strategijom i pratećim akcionim planovima. Na taj način će vršiti analize i davati mišljenja i preporuke, u skladu sa svojim nadležnostima, dok će jednom godišnje Vladi Crne Gore podnositi izvještaj o radu.
Kada je u pitanju kritična informatička struktura Crne Gore, na osnovu Startegije sajber bezbjednosti 2013-2017 donijete su Izmjene i dopune zakona o informacionoj bezbjednosti („Sl. list CG“, br. 40/16), gdje je definisana Kritična informatička infrastruktura i na osnovu toga prepoznato osam kritičnih sektora. Procesom zaštite KII upravlja država Crna Gora i ovaj model upravljanja predstavlja jedan od dva modela upravljanja u Evropskoj uniji. Krovno tijelo za koordinaciju aktivnosti, razvijanje saradnje i dugih djelatnosti u oblasti sajber bezbjednosti predstavlja Nacionalni CIRT.

U narednom periodu, Vlada Crne Gore će nastaviti da jača kapacitete za sajber odbranu KII, kroz obezbjeđivanje adekvatnih resursa i alata za razumijevanje, analizu i odgovor na prijetnje od strane Nacionalnog CIRT-a i drugih državnih organa koji su zaduženi za kontrolu bezbjednosti KII.

Ovom strategijom prepoznato je ukupno osam ciljeva za unaprjeđenje nacionalne sajber odbrane Crne Gore za period 2018-2021. godine, i to:

1. oslanjanje na evropske i evroatlantske koncepte,
2. snaženje kapaciteta za sajber odbranu,

3. centralizacija sajber ekspertize i resursa,
4. snaženje međuinstitucionalne saradnje,
5. zaštita podataka,
6. edukacija u oblasti sajber bezbjednosti,
7. jačanje partnerstava javnog i privatnog sektora, i
8. snaženje regionalne i međunarodne saradnje.

Crna Gora će kroz jasno definisane strateške ciljeve razviti potpuno kompatibilan koncept sa konceptima najrazvijenijih zemalja članica EU i NATO. Ovakav koncept će stvoriti preduslov za bezbjednije informaciono društvo i omogućiti uspješnu implementaciju Strategije sajber bezbjednosti i postojeće pravne regulative koja tretira ovu oblast.

U cilju jačanja kapaciteta za sajber bezbjednost, Vlada Crne Gore će nastaviti da se sa velikom pažnjom odnosi prema obezbjeđivanju dodatnih ljudskih i finansijskih resursa i drugih potreba institucija koje aktivno rade na bezbjednosti sajber prostora Crne Gore.

Aktivnosti na centralizaciji sajber ekspertize i resursa će omogućiti jačanje kapaciteta za odgovor na prijetnje po kritičnu informacionu infrastrukturu i druge sisteme koje su od državnog značaja, razumijevanje rizika po sajber prostor Crne Gore, pružanje adekvatnih preporuka i podspiješiti saradnju između javnog i privatnog sektora.
Takođe, Crna Gora će jačati nacionalne kapacitete potrebne za sprovođenje bezbjednosne akreditacije komunikaciono-informacionih sistema i procesa u kojima se koriste tajni podaci, kao i kapacitete u oblasti kriptografske zaštite podataka.

Nadležne institucije će aktivno raditi na jačanju međuinstitucionalne saradnje, kroz efikasnu i pravovremenu razmjenu informacija i najboljih praksi, organizaciju vježbi i simulacija napada većih razmjera. Na taj način će se definisati jasne procedure komunikacije u kriznim situacijama i uočiti nedostaci, koji će se pravovremeno otklanjati.

Regionalna i međunarodna saradnja predstavljaju važan segment u obezbjeđivanju nacionalne sajber bezbjednosti, pa će Crna Gora nastaviti sa regionalnim i međunarodnim aktivnostima i ulagati u partnerstva, u cilju unaprjeđenja i širenja ekonomskih i bezbjednosnih interesa, kao i poboljšanja kolektivne bezbjednosti.

Vlada Crne Gore će preduzeti dalje korake u cilju podizanja svijesti o problemu sajber bezbjednosti kako kod institucija i organizacija, tako i kod građana. Podizanje svijesti kroz informisanje o tome šta treba učiniti da bi se zaštitili prilikom rada na internetu će dovesti do cjelokupne promjene u ponašanju i obezbijediti da svi budu svjesni sajber bezbjednosti i načina zaštite kod kuće, u školi i na poslu.

U narednom periodu će biti nastavljeno sa radom na jačanju partnerstva između javnog i privatnog sektora, u cilju podrške u dijeljenju informacija,

pokretanja zajedničkih inicijativa i odgovora na incidente. Javno-privatno partnerstvo predstavlja efikasan način da se razumije i na pravi način odgovori na potrebe i izazove privatnih kompanija, a u cilju preduzimanja neophodnih mjera i postizanja dovoljnog stepena bezbjednosti.

Prema tome, bezbjednost sajber prostora Crne Gore je od presudnog značaja za ukupnu bezbjednost države i njenih građana. Većim angažovanjem predstavnika javnog, privatnog, akademskog i civilnog sektora u narednom periodu biće dat doprinos u obezbjeđivanju sajber bezbjednosti.

Bezbjedan sajber prostor, u konačnom, podstiče povoljan ambijent za dalji razvoj i napredak, na zadovoljstvo svih građana.

ANEKS: Definicije i termini

Aktivna sajber odbrana – princip implementiranja bezbjednosnih mjera za jačanje bezbjednosti mreže ili sistema kako bi bili otporniji na napade.

Autentifikacija – proces verifikacije identiteta ili drugih atributa korisnika, procesa ili uređaja.

Autonomni sistem – skup IP mreža čije rutiranje je pod kontrolom određenog entiteta ili domena.

Ažuriranje – proces instaliranja softvera sa ciljem popravke grešaka i ranjivosti.

Bitkoin (*eng. bitcoin*) – digitalna valuta i sistem za plaćanje.

Domen Sistem (*DNS*) – sistem mapiranja numeričke IP adrese na domen.

Domen – Domen locira organizaciju ili drugi entitet na internetu sa jedinstvenim imenom koje je registrovano u autorizovanim institucijama, tzv. domen registratorima.

Enkripcija – kriptografska transformacija podataka („običnog teksta“) u oblik („šifrovani tekst“) koji skriva orginalno značenje podataka, kako bi spriječili njihovo otkrivanje ili korišćenje.

E-trgovina – elektronska trgovina. Trgovina sprovedena ili omogućena putem interneta.

Industrijski kontrolni sistem – informacioni sistem koji se koristi za kontrolu industrijskih procesa, kao što su proizvodnja, rukovanje proizvodima i distribucija, ili za kontrolu infrastrukturnih sredstava.

Insajder – neko ko ima pristup podacima i informacionim sistemima organizacije i može predstvaljati prijetnju.

Integritet informacija – svojstvo da informacije nisu slučajno ili namjerno izmijenjene, da su tačne i potpune.

Internet – globalna računarska mreža, koja pruža razne informacione i komunikacione kapacitete, a koja se sastoji od međusobno povezanih računarskih mreža koristeći standardizovane komunikacione protokole.

Internet stvari – fizički uređaji (automobili, zgrade, televizori, kamere ...) koji sadrže elektroniku, softver i senzore i koji komuniciraju i razmjenjuju podatke putem interneta i imaju IP adresu.

Izviđanje (*eng. reconnaissance*) – faza napada kada napadač prikljupa informacije i mapira mreže, kao i ispitivanje ranjivosti sa ciljem kasnijeg upada u sistem.

KII – Kritična informatička infrastruktura

Korisnik – osoba, organizaciona jedinica ili automatizovani proces koji

pristupa sistemu bez obzira da li je ovlašćen ili nije.

Krađa podataka – neovlašćeno pomjeranje ili otkrivanje informacija na mreži onome koji nije ovlašćen da ima pristup ili uvid u informacije.

Kriptografija – nauka ili izučavanje analize i dešifrovanje kodova i šifara, kriptoanaliza.

Malver – maliciozni softver ili kod. Malver uključuje viruse, crve, trojance ili špijunski program (*eng. spyware*).

Odgovor na incident – aktivnosti koje se odnose na odgovor na kratoročne, direktne efekte nekog incidenta, a takođe mogu podržati kratoročni oporavak.

Penetracijsko testiranje – aktivnosti koje su dizajnirane da testiraju otpornost mreže ili objekata od hakovanja, a odobreno je ili sponzorisano od strane organizacije koja se testira.

Računarska mreža – skup računara, zajedno sa podmrežom ili mrežom, preko koje se mogu razmjenjivati podaci.

Ransomver – zlonamjerni softver koji kriptuje korisničke podatke i na taj način ih čini nedostupnim vlasnicima. Za povraćaj podataka traži se otkup.

Ranjivost – greške u softverskim programima koje mogu biti iskorišćene od strane napadača.

Rizik - mogućnost da će određena sajber prijetnja iskoristiti ranjivost informacionih sistema i nanijeti štetu.

Ruter – uređaj koji međusobno povezuje logične mreže prenošenjem informacija ka drugim mrežama u skladu sa IP adresama i protokolima.

Sajber bezbjednost – zaštita sistema, povezanih na internetu (uključujući hardver, softver i povezanu infrastrukturu), podataka na njima i usluga koje oni pružaju, od neovlašćenog pristupa, štete ili zloupotrebe. Ovo uključuje štetu prouzrokovanu namjerno od strane operatora sistema, ili slučajno, kao rezultat neizvršenja bezbjednosnih procedura ili štete koja je proizvod manipulacije.

Sajber incident – događaj koji zapravo ili potencijalno predstavlja prijetnju računaru, uređaju koji je povezan putem interneta ili mreže - ili podatke obrađivane, čuvane ili prenijete na tim sistemima - što može zahtijevati odgovor sa ciljem ublažavanje posljedica.

Sajber kriminal – krivična djela zavisna od sajbera (krivična djela koja se mogu izvršiti samo upotrebom ICT uređaja, gdje su uređaji i sredstvo za izvršenje krivičnih djela i meta krivičnih djela); ili krivična djela potpomognuta sajberom (krivična djela koja mogu biti počinjenja bez ICT uređaja, poput finansijskih prevara, ali se značajno mijenjaju korišćenjem ICT-a u smislu razmjera i dometa).

Sajber otpornost – sposobnost sistema i organizacija da izdrže sajber incidente i oporave se od štete u slučaju istih.

Sajber prijetnja - sve što može ugrožavati bezbjednost ili izazvati štetu na informacionim sistemima i internet konektovanim uređajima (uključujući hardver, softver i prateću infrastrukturu) podatke o njima i uslugama koje pružaju prvenstveno putem sajber sredstava.

Sajber prostor – međusobno povezana mreža informatičke infrastrukture koja uključuje internet, telekomunikacione mreže, računarske sisteme, internet povezane uređaje i ugrađene procesore, i kontrolere. Može se odnositi i na virtuelni svijet ili domen kao doživljeni fenomen ili apstraktni koncept.

Sajber-fizički sistem – sistemi sa integrisanim računarskim i fizičkim komponentama u kojima računari kontrolišu fizičke funkcije (tzv. „pametni“ sistemi).

SMS prevara – tehnika koja maskira porijeklo tekstualnih poruka zamjenjujući originalni mobilni broj (ID pošiljaoca) sa alfanumeričkim tekstom. Pošiljalac legitimno može svoj mobilni broj da zamijeni svojim imenom, ili nazivom poslovnog subjekta. Može se koristi i nelegitimno za lažno predstvaljanje.

Socijalni inženjering – metode koje napadači koriste kako bi prevarili ili izmanipulisali žrtvu da obavi određene akcije ili otkrije povjerljive informacije. Obično, takve akcije uključuju otvaranje zlonamjernih veb stanica ili neželjenih priloga.

Upravljanje incidentima – upravljanje i koordinacija aktivnosti za istraživanje i sanaciju, stvarnih ili potencijalnih neželjenih sajber događaja, koji mogu ugroziti ili uzrokovati štetu na sistemu ili mreži.

Virus – virusi su zlonamjerni računarski programi koji se mogu širiti na druge fajlove.