Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

NACIONALNA PLATFORMA REPUBLIKE SEVERNE MAKEDONIJE ZA IZGRADNJU SAJBER BEZBEDNOSTI

Pregledni naučni rad

Sašo MITEVSKI, Phd[415]
Blagojčo SPASOV, MA.[416]

SAŽETAK

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): U okviru savremenog sveta, kao i u mnogim državama u svetu, Republika Severna Makedonija nije imuna na savremene rizike i pretnje. Posebna meta ugrožavanja predstavlja sajber infrastruktura objekata od bitnog značaja za bezbednost države koji su svakodnevno predmet napada različitih kriminalnih struktura.
Ciljevi rada (naučni i/ili društveni Fokus istraživanja koje će biti sprovedeno obuhvatiće sajber bezbednost i sajber kriminal u Republici Severnoj Makedoniji kao savremeni oblik savremenog ugrožavanja.
Metodologija/Dizajn: Istraživanje, utvrdiće indikatore koji ukazuju na pojavu i širenje sajber napada u Republici Severnoj Makedoniji poslednjih nekoliko godina kao i utvrđivanje sposobnosti bezbednosnog sistema da se suoči sa ovom vrstom savremenih pretnji, preko analize nacionalne strategije i zakonske regulative koja određuje ovu vrstu ugrožavanja.
Ograničenja istraživanja/rada: Počevši od činjenice da je Republika Severna Makedonija cilj savremenih oblika ugrožavanja preko različitih formi sajber napada, postoji potreba od ozbiljnog pristupa i ozbiljnog istraživanja faktora koji omogućuju pojavu i širenje sajber kriminala u Republici Severnoj Makedoniji.
Rezultati/Generalni zaključak: U analizi koja je napravljena prema dostupnoj literaturi koja određuje bezbednost, javna bezbednost je predstavljena kao funkcija države koja garantuje zaštitu građana, institucija i organizacija od rizika pretnje institucija i organizacija od rizika i pretnji njihovom funkcionisanju, blagostanju i postojanju.
Opravdanost istraživanja/rada: Opravdanost istraživanja se ogleda u potrebi da se prizna važnost uspostavljanja nacionalne platforme Republike Severne Makedonije za izgradnju sajber bezbednosti.

Ključne reči
sajber kriminal, sajber zaštita, bezbednost, nacionalna strategija, kritična infrastruktura

[415] Ministarstvo Unutrašnjih poslova Republike Severne Makedonije Saso_Mitevski@moi.gov.mk
[416] Ministarstvo Unutrašnjih poslova Republike Severne Makedonije blagojcospasov@yahoo.com

ABSTRACT

Within the modern world, like many other countries in the world, the Republic of North Macedonia is not immune to contemporary risks and threats. A special target of threat is the cyber infrastructure of facilities vital to the security of the state that are subject to attacks from various criminal structures on a daily basis.

Starting from the fact that the Republic of North Macedonia is a target of modern forms of endangerment through various forms of cyber attacks, there is a need for serious approach and serious research into the factors that enable the emergence and spread of cybercrime in the Republic of North Macedonia.

The focus of the research that will be conducted will include cyber security and cybercrime in the Republic of North Macedonia as a modern form of modern endangerment.

The survey will determine the indicators that indicate the emergence and spread of cyber attacks in the Republic of North Macedonia in the last few years, as well as determining the ability of the security system to deal with this type of contemporary threats by analyzing the national strategy and legislation that Determines this type of endangerment.

Key words

cyber crime, cyber security, security, national strategy, critical infrastructure.

UVOD

Ugrožavanje sajber bezbednosti danas ide u korelaciji sa brzim razvojom visoke tehnologije koja pravi komjuterske sisteme vrlo ranljive. Sajber zakane se svakim danom više i više nameću kao savremeni problem, zahvaljujući faktu da vladine i javne službe, industrije, delovni subjekti i finsnsijske institucije, se sve više temelje na informatičku mrežnu povezanost to jest korišćenje digitalnih podataka i prenos informacija.

Društva se grade na osnovu složenih kompjuterskih mreža i sistema koji praktično upravljaju ukupnom kritičnom infrastrukturom u državi. Upravo to podiže stepen rizika neovlšćenog pristupa, zloupotrebe i uništavanje informacija od strane širokog sprektra zainteresovanih strana.

Uobičajeno, ove kompjuterske napade vrše bivši radnici u postojećim kompanijama, vladini i nevladini subjekti kao i terorističke formacije ali i anonimni i nezavisni hakeri. Globalne kriminalne mreže stiču sve veću sposobnost da prodru u računarske sisteme podataka, gde su skaldirani ogroman broj suštinskih informacija, da bi ih preuzeli i neovlšćeno koristili. Prodiranje u kompjuterske sisteme daje kriminalcima priliku da pristupe i iskoriste sve dostupne lične, finansijske, komercijalne i vladine podatke. Sve to ostavlja prostor za manipulaciju sa najosjetljivijim segmentima u svakom društvu. Pojava komjuterskih virusa već omogućava potpuno narušavanje integriteta informatičkog sistema.

Korišćenje termina sajber bezbednost ne znači samo hakovanje računarskih sistema, krađu ili zloupotrebu ličnih podataka. U današnjem razvijenom svetu, ugrožavanje sajber bezbednosti, dovodi do direktne pretnje po nacionalnoj sigurnosti svake države. Ranjivost država u smislu sajber bezbednosti je činjenica da je ukupna kritična infrastruktura u jednom modernom društvu povezana sa nacionalnom ili međunarodnom kompjuterskom mrežom. To je dovoljan pokazatelj osjetljivosti i ranjivosti nacionalnih kapaciteta u smislu sajber pretnji. Nema potrebe da se komentariše šteta koja bi rezultirala javnom ili nacionalnom bezbednošću kao rezultat zanemarivanja ili nedovoljne izgradnje sajber bezbednosti u društvu.

Dosad navedene informacije predstavljaju jednu ozbiljniju potrebu za istraživanjem koje će se tumačiti kroz sadržaj ovog rada, a radi se o analizi i određivanju načina na koji se sajber bezbednost gradi i održava u Republici Severnoj Makedoniji i u Evropskoj uniji. Polazeći od osetljivosti i aktuelnosti ove predmetne problematike ovog naučnog istraživanja, rezultati koji će biti dobiveni biće plasirani u okviru Republike Severne Makedonije i šire kako bi doprineli razmeni iskustava i građenje kapaciteta za suočavanje sa sajber pretnjama i regionu pa i šire.

1. TERMINOLOŠKA DIVERGENCIJA POJMOVA BEZBEDNOSTI, SAJBER BEZBEDNOSTI, KOMPJUTERSKI KRIMINAL

Bezbednosna situacija je složeni fenomen koji daje pregled obema i intenziteta više elemenata koji zagrožavaju nacionalnu bezbednost (opasnosti, rizici i izazovi), koji u određeno vreme pojedinačno ili kombinovano utiču na bezbednost građana, zajednica ili specifične pretnje čak i državi. Bezbednosna situacija se sadrži od više faktora ili indikatora. Oni pokazuju kakva je bezbednosna situacija u vezi sa pitanjima javnog reda i mira, dinamika kriminala (koji utiče na ličnu bezbednost, bezbednost stečenih materijalnih dobara građana i društvene svojine), uticaj stranih elemenata na unutrašnju bezbednost, pretnje od ekstremističkih organizacija, razvoja bezbednosnih dešavanja u regionu i svetu, međunarodnih odnosa zemlje i drugih (Rajkovcevski, 2014).

Jedna od osnovnih funkcija države za postizanje svojih ciljeva je bezbednosna funkcija. Funkcija bezbednosti je prisutna od samog nastanka države, koja se konstantno razvija i usavršava (Dončev, 2007).

U analizi koja je napravljena prema dostupnoj literaturi koja određuje bezbednost, javna bezbednost je predstavljena kao funkcija države koja garantuje zaštitu građana, institucija i organizacija od rizika pretnje institucija i organizacija od rizika i pretnji njihovom funkcionisanju, blagostanju i postojanju (Mijalković, 2011).

Bezbednost kao fenomen, odnosno njeno tumačenje je veoma složeno i kompleksno, što omogućava postojanje različitih mišljenja i interpretacija ovog pojma (Kotovčevski, 2011).

Termin sajber bezbednost odnosi se na bezbednost u sajber prostoru a to je prostor (informatička mreža) koji je potreban da bi ta sajber bezbednost funkcionisala. Sajber spejs podrazumeva sve ono što se odnosi na komjutere, internet, mobilne uređaje i ostale pametne uređaje koji su vezani u nekoj mreži. Sajber prostor je pun kritičnih informacija neovisno o tome da li su to nečija privatna svojina ili svojina neke vladine institucije. Današnji načini komunikacije podrazumeva nezamislivo veliku razmenu podataka i informacija preko sajber prostora. Zbog toga bezbednost ovih informacija je od suštinskog značaja za njihovo prenošenje od početne tačke do krajnog korisnika.

Grupa renomiranih autora definiše ovaj komjuterski kriminal u užem i širem smislu, gde u užem smislu navode kompjuterske prevare, sabotaže, špijuniranja, a u šire značenje odnosi se na zloupotrebu kompjutera i njegovih komponenti od krađe, pronevere i slično (Šarkić, i ostali, 2011).

Autor Spasić., u svojoj definiciji o sajber kriminalu navodi da se radi o zločinu koji se odvija u digitalnom okruženju i predstavlja specifičan oblik nezakonitog ponašanja u kojem se računarska mreža pojavljuje kao sredstvo, meta ili dokaz za izvršenje krivičnog dela (Spasić, 2006).

Ulazak u kompjuterske sisteme daje kriminalcima mogućnost da pristupe i manipulišu ličnim, finansijskim, komercijalnim i vladinim podacima. Uvođenje kompjuterskih virusa može sasvim narušiti integritet sistemu sa podacima (Lajman.D.M., Poter.V.G, 2009).

U dostupnoj literaturi u kojoj ovi termini gravitiraju, može se odrediti razlika od nesuštinskog značaja u definiranju pojmova bez promene njenog pravog istinitog značaja.

2. MEHANIZMI EVROPSKE UNIJE ZA GRAĐENJE SAJBER BEZBEDNOSTI

Sajber bezbednost je od ključnog značaja za evropski prosperitet i evropsku bezbednost, sa razlogom da svakodnevni život i evropska ekonomija sve više zavise od digitalnih tehnologija. Incidenti u sajber bezbednosti su raznoliki iz aspekta ko je odgovoran i šta sa tim incidentima želi da postigne. Naglašene sajber aktivnosti ne samo da ugrožavaju evropsku ekonomiju, već su i usmerene prema digitalnom jedistvenom tržištu, a prodiru i u funkcionisanje evropske demokratije, slobode i vrednosti. Evropska bezbednost zavisi od stepena sposobnosti relevantnih nadležnih službi sa obzirom na činjenicu da se, civilna infrastruktura i vojni kapaciteti, oslanjaju na sigurne digitalne sisteme (EU Global strategy, II, 2018).

U mnogim izveštajima Evropske komisije zabeleženo je da sajber bezbednost u Evropskoj uniji može biti ugrožena od strane nedržavnih i državnih subjekata. Ugrožavanja sajber bezbednosti najčešće imaju krivičan, politički i strateški cilj, ali najradije je reč je o ugrožavanju zbog sticanja brze zarade i lakog profita. Kriminalni aspekat se pojačava približavanjem granice između kompjuterskog kriminala i "tradicionalnog" kriminala, budući da

kriminalci koriste internet kao način na koji povećavaju svoje aktivnosti, a isto tako i kao izvor za pronalaženje novih metoda i sredstava za izvršenje krivičnih djela. Evropsko iskustvo kaže da su u mnogim slučajevima šanse za praćenje kriminala minimalne, a šanse za krivično gonjenje još manje (European commission, 2017).

Mrežne infiltracije u tuđim kompjuterskim sistemima dovode do nezakonitog pristupa, objavljivanje privatnih podataka (povrede podataka) ili intelektualne svojine. Kao takvi su u stalnom porastu a, spominje se brojka od stotinu milijona zapisa globalno ugroženih svake godine. Kompromitovani podatci mogu se koristiti za razne kriminalne svrhe, uključujući prevaru i iznudu. Neke zemlje - članice potenciraju da su česta meta napada sektori ili mreže koje imaju podatke koji mogu biti "dobra zaradnja" (SOCTA, 2017).

Ovi državni i nedržavni subjekti koji postoje, deluju na području Evrope, sve više ispunjavaju svoje geopolitičke ciljeve ne samo korištenjem klasičnih alata kao vojne sile, već i putem sofisticiranih sajber alata, čime omogućavaju i mešanje u unutrašnje demokratske procese pojedinih zemalja. Korišćenje sajber - prostora kao domen ratovanja, bilo sam, ili kao deo hibridnog pristupa, sada je široko prihvaćen. Kampanje o dezinformacijama, lažnim vestima i sajber operacijama usmerene prema kritičnoj infrastrukturi su sve češće i zahtevaju odgovore. Iz tog razloga, u dokumentu u kome je tema razmišljanje o budućnosti evropske odbrane, neophodna je potreba za saradnju između nadležnih subjekta u državama u oblasti sajber odbrane (SOCTA: 2017).

U izveštaju Evropske komisije od 13.09.2017. godine, stoji da će se sajber rizik povećavati u suglasnosti sa digitalnim transformacijama. Očekuje se da će desetine milijardi uređaja sa "Internet stvarima" biti povezane na internet do 2020. godine, ali sajber bezbednost još uvek nije prioritet u njihovom dizajnu. Neuspeh proizvođača da zaštite uređaje koji će kontrolisati naše električne mreže, automobile i transportne mreže, fabrike, finansije, bolnice i domove mogu imati katastrofalne posledice i naneti veliku štetu poverenju potrošača u novim tehnologijama. Rizik od politički motivisanih napada na civilne ciljeve, kao i nedostatci u vojenoj sajber odbrani, još više produbljuju rizik (European commission: 2017).

Agencija Evropske unije za bezbednost mreža i informacija (ENISA) igra ključnu ulogu u jačanju sajber otpora u odgovorima na na temi sajber bezbednost Evropskoj uniji. Ona aktivno doprinosi u uspostavljanju visokog nivoa mrežne sigurnosti i informacija unutar Unije, od kada je osnovana od 2004. godine. Ona takođe doprinosi razvoju kulture bezbednosti mreže i informiranja u društvu i kako bi se podigla svest o bezbednosti o informacijama i mrežama, što zauzvrat dovodi do pravilnog funkcionisanja unutrašnjeg tržišta. Agencija u biti sarađuje sa zemljama – članicama i privatnim sektorom, gde daje savete i rešenja. Ona organizuje pan-evropske sajber-bezbednosne vežbe, razvoj nacionalne sajber-bezbednosne strategije i građenje kapaciteta, ali isto tako radi i studije za bezbedno prihvatanje i rešavanje pitanja vezana za zašitu podataka, tehnologije za poboljšanje privatnosti i privatnost novih tehnologija, identifikovanje sajber pretnje, pejzaže i drugo.

ENISA ujedno podržava razvoj i sprovođenje politike i zakona Evropske unije po pitanjima vezana sa bezbednosti mreža i informacija (ENISA: 2019).

Da bi poboljšao učinak agencije, Evropska komisija je predstavila ambiciozan predlog reforme, uključujući i stalni mandat za agenciju. Reforma će omogućiti agenciji da pruži podršku državama članicama, institucijama i preduzećima Evropske unije u ključnim oblastima, uključujući implementaciju Direktive o mrežnoj sigurnosti i informacionim sistemima i predloženog okvira za sertifikaciju sajber-bezbednosti (Directive 1148: 2016).

Reforma će omogućiti agenciji da ima snažnu savetodavnu ulogu u razvoju i implementaciji politika, uključujući promoviranje koherentnosti između sektorskih inicijativa i Direktive o sigurnosti i mreži, kao i pomoć u uspostavljanju centra za razmenu informacija i analiza u kritičnim sektorima. Očekuje se da će Agencija ojačati evropsku spremnost organiziranjem godišnjih pan-evropskih sajber bezbednosnih vežbi kombinirajući odgovor na različnom nivou. Takođe će podržati razvoj sertifikacije Evropske unije o sajber bezbednosti za politiku informacionih i komunikacionih tehnologija (IKT) i igraće važnu ulogu u jačanju operativne saradnje i upravljanje krizama širom Evropske unije. Agencija će također služiti kao žarišna točka za informacije i znanje u zajednici za kibernetičku sigurnost (European commission: 2017).

Na osnovu navedenih incidenata koji proizlaze iz sajber-bezbednosti mogli bi značajno uticati na funkcionisanje kritične infrastrukture Evropske unije kao i na svakodnevni život ljudi, tako da postoji potreba da se utvrdi mogućnost uspostavljanja tela za reagovanje u vanrednim situacijama koje izaziva sajber napad. Ovo telo može biti formirano koristeći model drugih alata Unije koji se pojavljuju iz upravljanja krizom, ali i drugih područja Evropske unije. Ovo će omogućiti državama članicama da traže pomoć na nivou Evropske unije tokom ili nakon velikog incidenta, pod uslovom da država članica uspostavi sistem sajber bezbednosti pre incidenta, uključujući punu implementaciju neophodnih direktiva, profesionalno upravljanje rizicima i nadzorne okvire na nacionalnom nivou. Takav fond, dopunjavajući postojeće mehanizme za upravljanje krizama na nivou Evropske unije, mogao bi primijeniti sposobnosti brzog reagovanja u interesu solidarnosti i finansirati specifične akcije reagiranja na katastrofe, kao što je zamjena ugrožene opreme ili primjena alata za ublažavanje ili odgovor, oslanjajući se na nacionalnu ekspertizu u skladu sa mehanizmom civilne zaštite Evropske unije (HIGH REPRESENTATIVE OF THE UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY: 2017).

Europol je agencija za sprovođenje zakona u Evropskoj uniji i pomaže državama članicama u borbi protiv teškog međunarodnog kriminala i terorizma. Osnovana kao agencija Unije u 2009 –toj godini, Europol ili Evropska policijska kancelarija je srce evropske bezbednosne arhitekture i nudi jedinstveni spektar usluga. Europol je centar za poddršku policijskim operacijama, informativni centar o zločinima i centar za ekspertizu za sprovođenje zakona. Analiza je srž aktivnosti Europola. Kako bi svojim partnerima pružio dublje znanje o zločinima s kojima se suočavaju, Europol vrši redovne procjene koje nude sveobuhvatne, progresivne analize kriminala i terorizma u Evropskoj uniji (SOCTA: 2017).

U cilju održavanja visoke sajber-bezbednosti, Europol kao nadležni organ Evropske unije za suočavanje sa teškim i organizovanim kriminalom u 2013. godine uspostavio je Evropski centar za kibernetički kriminal kako bi ojačao implementaciju zakona o sajber kriminalu u Evropskoj uniji i na taj način pomoći u zaštiti evropskih građana, preduzeća i vlada od kriminala na internetu. Od svog osnivanja, Evropski centar za kibernetički kriminal je dao značajan doprinos borbi protiv sajber kriminala, bio je uključen u desetine operacija visokog profila i stotine operativnih priključaka, što je rezultiralo stotinama hapšenja i analizom stotina hiljada datoteka, od kojih je većina pokazala se zaraženom. Prema Evropskom centru za kibernetički kriminal, iako je teško dati pouzdane procene, neki izvještaji u industriji pokazuju da su globalni troškovi kibernetičkog kriminala stotine milijardi eura godišnje. Evropski centar za kibernetički kriminal svake godine objavljuje procenu pretnje s Interneta za organizirani kriminal putem strateškog izvještaja o ključnim nalazima i novim pretnjama i zbivanjima u oblasti kibernetičkog kriminala. Strateški izvještaj pokazuje koliko je širok i raznolik kompjuterski kriminal i kako je Evropski centar za kibernetički kriminal ključni deo Europola i odgovor EU. Evropski centar za kibernetički kriminal ima trostruki pristup u borbi protiv sajber kriminala: forenzike, strategije i operacije (EUROPOL: 2019).

U Evropskoj uniji postoji osećaj da će digitalizacija i povezivanje doneti veće rizike od kibernetičkog kriminala, što čini celim društvom osjetljivijim na kibernetičke pretnje, a osim društva i građana, oni se suočavaju sa sve većim opasnostima, uključujući ugrožene kategorije kao što su deca. Da bi se ovaj rizik ublažio društvu, evropske zemlje moraju preduzeti sve neophodne mere za poboljšanje sigurnosti u Uniji, kako bi bolje zaštitile mrežne i informacijske sisteme, telekomunikacijske mreže, digitalne proizvode, usluge i uređaje koje koriste građani, vlade i nevladine organizacije.

3. NACIONALNA STRATEGIJA REPUBLIKE SEVERNE MAKEDONIJE ZA SAJBER BEZBEDNOST

Republika Severna Makedonija je u proteklom periodu uložila ogromne napore da ojača sajber bezbjednost svojih građana, svojih nacionalnih kapaciteta i kritične infrastrukture. U tom pravcu, analiziran je veliki broj međunarodnih iskustava i sproveden je veći broj studijskih poseta u mnogim zemljama Evropske unije i šire u oblasti sajber bezbednosti. Koristeći dobijene informacije, na osnovu bogatog međunarodnog iskustva, stručnjaci iz oblasti Severne Makedonije doneli su Nacionalnu strategiju kibernetičke sigurnosti za period 2018-2022. godine i Akcioni plan za implementaciju Nacionalne strategije, koji su bili ključni dokumenti za poboljšanje sajber bezbednosti u državi za duži vremenski period. Nacionalna strategija pokriva sajber izazove i trendove, određuje principe sajber bezbednosti, definiše viziju, misiju i ciljeve nacionalne strategije, odnosno uspostavlja metodologiju za njihovu implementaciju u pravcu izgradnje sajber bezbednosti u Republici Severnoj Makedoniji. Postojanje strateških dokumenata vezanih za ovaj izazov je ključno u naporima za jačanje kapaciteta u oblasti sajber bezbednosti. Razvoj Nacionalne strategije za sajber bezbednost ima primarnu funkciju za poboljšanje okvirnih uslova u ovoj oblasti.

Potreba za razvojom i usvajanjem Nacionalne strategije za kibernetičku sigurnost uglavnom se odnosi na sljedeće: (NSSB 2018-2022: 2019).

1. Aktivnosti, društvene interakcije, ekonomija, kao i osnovna ljudska prava i slobode usko su povezani sa primenom informacionih i komunikacionih tehnologija, zbog čega je neophodno obezbediti otvoren, siguran i bezbedan sajber prostor;
2. Upotreba sistema informacionih i komunikacionih tehnologija i razvoj elektronskih usluga povećava rizik od sajber nezgoda i zloupotreba, čineći ove pretnje ozbiljnijim u pogledu na nacionalnu bezbednost;
3. Definiranje i razvoj politike sajber odbrane;
4. Uspostaviti integrirani, multidisciplinarni pristup kako bi se osigurala bliža saradnja i koordinacija između sektora odbrane i sigurnosti, institucija uključenih u borbu protiv sajber kriminala, privatnog sektora, građana i građanskih organizacija civilnog društva, kao i drugih relevantnih strana;
5. Jačanje operativnih kapaciteta, koordinacije i saradnje između relevantnih institucija i organizacija uključenih u borbu protiv sajber kriminala;
6. Uspostaviti zajedničke standarde, obuku i obrazovanje svih institucija i organizacija uključenih u razvoj sajber bezbednosti;
7. Jačanje institucionalnog i pravnog okvira u oblasti sajber bezbednosti;
8. Jačanje nacionalnih kapaciteta za prevenciju i zaštitu od sajber napada, kao i sprovođenje aktivnosti usmjerenih na podizanje nacionalne svesti o sajber bezbednosti.

Nacionalna strategija za poboljšanje sajber bezbednosti može se posmatrati kroz prizmu tekućih reformi u Republici Severnoj Makedoniji koje su u poslednjih nekoliko godina provedene u sferi sigurnosno-obavještajne zajednice. U ovoj oblasti već postoji u nacionalnom zakonodavstvu Operativna tehnička agencija OTA koja praktično proizilazi iz procesa reforme koji se provodi u Upravi za bezbednost i kontraobavještajne poslove pri Ministarstvu unutrašnjih poslova. Izgradnja nacionalne strategije za sajber bezbednost i implementaciju svih reformskih procesa u ovoj sferi predstavlja veliki korak napred za Republiku Severnu Makedoniju u njenim severnoatlantskim aspiracijama prema Evropskoj uniji.

Razvoj bezbednog društva i primena svih bezbednosnih praksi i procesa kroz saradnju svih zainteresovanih strana će obezbediti da preduzeća ostanu poverljiva i pristupačna korisnicima, i stoga profitabilna. Povećanje povjerenja građana u digitalne usluge i elektronsku trgovinu direktno će doprinijeti razvoju digitalne ekonomije. To će doprineti u prepoznavanju Republike Severne Makedonije kao sigurnog mesta za investicije i poslovanje (NSSB 2018-2022: 2019).

4. ZAKONSKA REGULATIVA U REPUBLICI SEVERNOJ MAKEDONIJI

U globalnom i regionalnom kontekstu, sajber pretnje predstavljaju opasan i moderan fenomen koji narušava opštu sigurnost u informativnoj sferi, čime se reflektirajuće ugrožava i javnost i nacionalna sigurnost. Kao takav, ovaj fenomen je pokriven krivičnim zakonom svake zemlje koja je usvojila mnoge zakone koji određuju mehanizme i načine zaštite od ovog globalnog fenomena. U Republici Severnoj Makedoniji, pretnje sajber bezbednošću najčešće se vrše kroz različite oblike kibernetičkog kriminala. Ove sajber pretnje se u zemlji smatraju novijim kriminalnim fenomenom koje se prema svojim karakteristikama razlikuju od drugih kriminalnih ponašanja, najčešće načinom kriminalne aktivnosti ili samog objekta krivičnog napada, gde su u većini slučajeva glavni cilj računarski sistemi i elektronski podaci.

Kompjuterizacija makedonskog društva stvara sve veću opasnost od njihove moguće zloupotrebe, što podrazumeva povećanje broja krivičnih dela u oblasti sajber sfere.

U nacionalnom zakonodavstvu u borbi protiv kompjuterskog kriminala u Republici Severnoj Makedoniji postoji Krivični zakonik, Zakon o praćenju komunikacija, Zakon o elektronskim komunikacijama i drugi relevantni zakoni.

Krivični zakonik u svom sadržaju određuje predmet u kojem je propisano sljedeće:[417]

1. Stavom 26. člana 122. propisano je da je kompjuterski sistem je bilo kakav uređaj ili grupa međusobno povezanih uređaja, od kojih jedan ili više obavlja automatsku obradu podataka u skladu sa određenim programom.
2. Stav 27. člana 122. propisuje da se pod terminom kompjuterski podaci podrazumevaju propisani fakti, informacije ili koncepti u obliku koji je pogodan za obradu putem kompjuterskog sistema, uključujući program sličan kompjuterskom sistemu za njegovo stavljanje u funkciju.

Član 149. odnosi se na zloupotrebu ličnih podataka kao što je predviđeno:[418]

1. Lice koje, suprotno uslovima utvrđenim zakonom bez saglasnosti građanina, prikuplja, obrađuje ili koristi tuđe lične podatke, biće kaznjen novčanom kaznom ili kaznom zatvora do jedne godine.
2. Kazna iz člana 149. stav 1. izriče se licu koje ulazi u informacioni sistem računara sa ličnim podacima koje ih namerno koristi za sebe ili za drugog da bi ostvarilo određenu korist ili prouzrokovalo štetu drugom.

---

[417] Krivični Zakon Republike Severne Makedonije, Službeni list, 80/99, 4/02, 43/03, 19/04, 81/05, 60/06, 73/06, 7/08, 139/08, 114/09, 51/11, 135/11 , 185/11, 142/12, 166/12, 55/13, 82/13, 14/14, 27/14, 28/14, 115/14, 132/14 (2019).
[418] Isto.

3. Ako je krivično delo iz stavova 1. i 2. ovog člana izvršeno od strane službenog lica u vršenju svoje dužnosti, kazniće se zatvorom od tri meseca do tri godine.
4. Pokušaj u vezi sa stavovima 1 i 2 takođe će biti kažnjiv.
5. Ako je delo iz ovog člana izvršeno od strane pravnog lica, kazniće se novčanom kaznom.
6. Šteta i neovlašćeni ulazak u kompjuterski sistem je takođe kažnjivo delo.

Član 251. ovog Zakona predviđuje:[419]

1. Lice koje neovlašćeno briše, menja, oštećuje, prikriva ili na drugi način čini neupotrebljive kompjuterske podatke ili program ili uređaj za održavanje informatičkog sistema ili otežava korišćenje komjuterskog sistema, podataka ili programa ili kompjuterske komunikacije, kazniće se novčanom kaznom ili kaznom zatvora do tri godine.
2. Stavom 4. člana 251. navodi se da će on / ona počiniti djela iz stavova (1), (2) i (3) ovog člana prema kompjuterskom sistemu, podacima ili programima zaštićenim posebnim zaštitnim merama ili korištenim u rad državnih organa, javnih preduzeća ili javnih institucija ili u međunarodnim komunikacijama ili kao član grupe koja je stvorena za vršenje takvih krivičnih dela, kazniće se zatvorom od jedne do pet godina.
3. Stav 1. člana 251-b propisuje: Osoba koja, sa namerom da pribavi nezakonitu imovinsku korist za sebe ili drugog, unoseći u računar ili informacioni sistem neistinite podatke, ne predstavljajući istinite podatke promenom, brisanjem ili suzbijanjem računarskih podataka, falsifikovanjem elektronskog potpisa ili na drugi način izazvati neistinit rezultat u elektronskoj obradi i prenosu podataka, kazniće se novčanom kaznom ili kaznom zatvora do tri godine.

Zakon o praćenju komunikacija proizilazi iz nacionalnog zakonodavstva koje ima veliki uticaj u smislu sprečavanja ugrožavanja sajber pretnji i definiše: proceduru za sprovođenje posebne istražne mere: praćenje i evidentiranje telefonskih i drugih elektronskih komunikacija, uslove i postupak za sprovođenje mera za praćenje komunikacija u cilju zaštite interesa sigurnosti i odbrane države, uključujući metapodatke, nadzor i kontrolu nad sprovođenjem mera monitoringa komunikacija, obaveza Operativno-tehnička agencija i telekom operateri.[420]

Prema članu 4. stav 7. ovog zakona, nadležni organi za sprovođenje mera za praćenje komunikacije radi zaštite interesa bezbednosti i odbrane države su: Ministarstvo unutrašnjih poslova - Uprava za bezbednost i kontraobaveštaj i Ministarstvo odbrane - Služba

[419] Isto.
[420] Zakon za praćenje komunikajcija, Službeni list RSM 71/18 (2019).

vojne bezbednosti i Inteligencija, a u delu frekvencijskog spektra radio-talasa na visokim, vrlo visokim i ultra visokim frekvencijama (HF, VHF i UHF), ovlašćeni organ za provođenje mjere za praćenje komunikacije je Centar za elektronski uvid Armije Republike Makedonije koji funkcioniše u službi odbrane države. Navedene vlasti su ovlašćene da sprovode mere za presretanje komunikacija u svrhu obavljanja delatnosti za koje su nadležne u skladu sa zakonom.[421]

Članom 18. ovog zakona definisane su mere praćenja komunikacija radi zaštite interesa sigurnosti i odbrane države: praćenje i evidentiranje telefonskih i drugih elektronskih komunikacija, praćenje i snimanje u unutrašnjosti zgrada, zatvorenih prostorija i objekata i ulazak u onim objektima, zatvorenim prostorijama i objektima, u cilju stvaranja uslova za sprovođenje mere, praćenja i svjetlosnog snimanja osoba na otvorenom prostoru i na javnim mestima i praćenja i audio snimanja sadržaja komunikacija osoba na otvorenom prostoru i na javnim mestima.[422]

Nalog za utvrđivanje mera za praćenje saopštenja iz člana 18. donosi nadležni sud u Republici Sjevernoj Makedoniji po prethodnom zahtevu nadležnih institucija koje imaju ovlaštenje za praćenje elektronskih komunikacija, odnosno Javnog Tužioca.

Imajući u vidu činjenicu da su informacije od vitalnog značaja za javnu i nacionalnu bezbednost u Republici Severnoj Makedoniji klasifikovanog karaktera, pomenut ćemo Zakon o klasificiranim informacijama koji je od suštinskog značaja za rešavanje sajber pretnji u smislu zaštite informacija sa stepenom klasifikacije zaštite informacija.

Svrha Zakona o klasifikovanim informacijama u Republici Severnoj Makedoniji je da se osigura zakonito korištenje tajnih podataka i da se spreči bilo kakav oblik nezakonitog pristupa informacijama, kao i da se utvrdi stepen zaštite informacija koje bi trebale odgovarati stepenu štete koja bi nastala za Republiku Severnu Makedoniju sa neovlašćenim pristupom ili neovlašćenim korišćenjem informacija. Informacije koje su predmet klasifikacije odnose se naročito na: javnu bezbednost; odbrane; inostrane poslove; bezbednosne, obaveštajne i kontraobaveštajne aktivnosti organa državne uprave Republike Makedonije; sistemi, uređaji, projekti i planovi od značaja za javnu bezbednost, odbranu, spoljne poslove; naučna i tehnološka, ekonomska i finansijska pitanja od značaja za Republiku Severnu Makedoniju.[423]

Zakon o elektronskim komunikacijama takođe ima veliki uticaj na izgradnju sajber bezbednosti u Republici Severnoj Makedoniji. Ovaj zakon predviđa: Podsticanje razvoja javnih elektronskih komunikacionih mreža i usluga u Republici Severnoj Makedoniji u cilju

---

[421] Isto.
[422] Isto.
[423] Zakon o klasifikovanim informacijama, Službeni list RSM, 09/04, 113/07, 145/10, 80/12, 41/14, 21/18 (2019).

osiguranja ekonomskog i društvenog razvoja; podsticanje korišćenja i razvoja širokopojasnog pristupa uslugama (broadband); zaštitu prava korisnika, uključujući krajnje korisnike sa invaliditetom i krajnje korisnike sa posebnim socijalnim potrebama; obezbeđivanje efikasne i održive konkurencije na tržištu elektronskih komunikacija; pružanje univerzalne usluge; efikasno korišćenje radiofrekvencijskog spektra i numeracije; promovisanje razvoja i podsticanje investicija u javne elektronske komunikacione mreže uvođenjem novih tehnologija i usluga, a posebno uvođenjem sledećih generacija javnih elektronskih komunikacionih mreža i obezbeđivanjem poverljivosti komunikacija.[424]

5. ULOGA MINISTARSTVA UNUTRAŠNJIH POSLOVA U SPREČAVANJU SAJBER PRETNJI

Ministarstvo Unutrašnjih Poslova u Republici Severnoj Makedoniji ima ključnu ulogu u ranom otkrivanju i suzbijanju sajber pretnji koje svakodnevno napadaju sajber strukture u Republici Sjevernoj Makedoniji. Nadležnosti Ministarstva unutrašnjih poslova proizilaze iz Zakona o unutrašnjim poslovima, Zakona o policiji i Zakona o presretanju komunikacija.

Prema Zakonu o unutrašnjim poslovima, Ministarstvo unutrašnjih poslova je odgovorno za: realizaciju sistema javne i državne bezbednosti; sprečavanje nasilnog rušenja demokratskih institucija utvrđenih Ustavom Republike Severne Makedonije; zaštitu života, lične sigurnosti i imovine građana; sprečavanje nanošenja nacionalne, rasne ili verske mržnje i netolerancije; sprečavanje izvršenja krivičnih dela i prekršaja, otkrivanje i hapšenje njihovih počinilaca i preduzimanje drugih mera propisanih zakonom za krivično gonjenje počinilaca tih dela; građanskim stvarima i drugim pitanjima utvrđenim ovim i drugim zakonima.[425]

Ministarstvo unutrašnjih poslova svoje nadležnosti obavlja preko Zavoda za javnu bezbednost i Direkcije za bezbednost i kontraobaveštajne poslove.

Preko Biroa za javnu bezbednost obavljaju se policijski poslovi, gde se u članu 5. Zakona o policiji predviđa: zaštita života, lične bezbednosti i imovine građana; zaštita sloboda i prava pojedinca i građana garantovanih Ustavom Republike Severne Makedonije, zakonima i ratifikovanim međunarodnim sporazumima; sprečavanje izvršenja krivičnih dela i prekršaja, otkrivanje i hapšenje njihovih počinilaca i preduzimanje drugih mera propisanih zakonom za krivično gonjenje počinilaca tih dela; utvrđivanje i traženje direktne i indirektne imovinske koristi stečene izvršenim krivičnim djelom; održavanje javnog reda i mira; regulisanje i kontrolu drumskog saobraćaja; kontrolu kretanja i boravka stranaca;

[424] Zakon o elektronskim komunikacijama, Službeni list RSM, 39/14, 188/14, 44/15, 193/15, 11/18, 21/18, (2019).
[425] Zakon o unutrašnjih poslova, Službeni list RSM, 42/14, 116/14,33/15 (2019).

granične kontrole i nadzor granica; pružanje pomoći i zaštita građana u slučaju potrebe; obezbjeđivanje određenih osoba i objekata i drugih aktivnosti utvrđenih zakonom. [426]

U okviru Biroa za javnu bezbednost postoji Odeljenje za prevenciju organizovanog i teškog kriminala, koje ima širok spektar nadležnosti i mehanizama za rano otkrivanje i sprečavanje sajber pretnji u zemlji, a ima i nadležnost da otkrije počinioce takvih nezakonitih radnji i njihovo lišavanje sloboda.

U prevenciji i suzbijanje sajber pretnji uključena su ministarstva unutrašnjih poslova, koja su sastavni dio Zavoda za unutrašnje poslove, gdje se redovnim policijskim stanicama pružaju redovne informacije građanima i njihovo upoznavanje s opasnostima koje proizlaze iz sajber zločina.

U Birou za javnu bezbednost kao zasebnu organizacisku strukturu postoji Sektor za kompjuterski kriminal i digitalnu forenziku, koji ima širok spektar nadležnosti u delu: (MUP RSM:2019).

- Efikasnu prevenciju;
- Otkrivanje počinilaca sajber kriminala;
- Pružanje odgovarajućih dokaza;
- Digitalnu forenziku;
- Krivično gonjenje počinilaca krivičnih dela;
- Pokretanje krivičnog postupka protiv počinilaca krivičnih dela u oblasti kompjuterskog kriminala;

Sektor za kibernetički kriminal i digitalnu forenziku je specijalizovana organizaciona struktura za borbu protiv ove vrste kriminala i trajno sarađuje sa regionalnim sektorima unutrašnjih poslova radi razmjene podataka i informacija za lica koja vrše ovu vrstu kriminala, pružanje stručne pomoći i direktno učešće u realizaciji potencijalnih slučajeva u koordinaciji sa Sektorom za unutrašnje poslove (MUP RSM: 2019).

Sektor za kibernetički kriminal i digitalnu forenziku takođe ima aktivnu međunarodnu saradnju u vezi sa Interpolovim i Europolovim odnosima, kao i sa drugim relevantnim međunarodnim bezbednosnim strukturama u cilju razmene informacija i ranog otkrivanja takvih zločina.

Uprava za bezbednost i kontraobaveštajnu službu iz člana 23. Zakona o unutrašnjim poslovima odgovorna je za vođenje unutrašnjih poslova vezanih za bezbednost i kontraobavještajnu delatnost koja se odnosi na: kontraobavještajnu delatnost; suzbijanje i zaštita od terorizma; zaštitu od drugih aktivnosti u cilju ugrožavanja ili prisilnog rušenja

[426] Zakon o policiji, Službeni list RSM, 114/06, 06/09, 145/12, 41/14, 33/15 (2019).

demokratskih institucija utvrđenih Ustavom Republike Severne Makedonije i težih oblika organizovanog kriminala koji potiču ili su usmjereni prema demokratskim institucijama sistema utvrđenih Ustavom Republike Sjeverne Makedonije i mogu dovesti do njihovog ugrožavanja ili uticaj na bezbednost države.[427]

Imajući u vidu gore navedeno, možemo zaključiti da Ministarstvo unutrašnjih poslova igra ključnu ulogu u prevenciji, otkrivanju i zadržavanju počinilaca kibernetičkog kriminala na teritoriji Republike Sjeverne Makedonije i šire putem razmene informacija i podataka sa nadležnim institucijama i agencijama na regionalnom i globalnom nivou.

ZAKLJUČNA SAGLEĐIVANJA:

1. Republika Severna Makedonija je potencijalna meta sajber napada, od raznih domaćih kriminalnih formacija, ali i od međunarodnih kriminalnih grupa;
2. Imajući u vidu da slučajevi sajber bezbednosti mogu značajno da utiču na funkcionisanje ekonomije, stabilnost i svakodnevni život ljudi, čini Republiku Severnu Makedoniju ranjivom u aspektu sajber bezbednosti;
3. Vlada Republike Severne Makedonije je razvila nacionalnu strategiju za sajber bezbednost za period 2018-2022;
4. Implementacija nacionalne strategije direktno zavisi od implementacije Akcionog plana za implementaciju strategije od strane Vlade RSM;
5. Evropske direktive o jačanju kapaciteta za bavljenje kibernetičkim pretnjama su veoma primenjive na implementaciju nacionalne strategije i takođe su obavezujući element za evroatlantske integracije Republike Severne Makedonije;
6. Nacionalna strategija za kibernetičku sigurnost mora se stalno nadograđivati u skladu sa nacionalnim prioritetima, direktivama i mehanizmima za sigurnost mreže i informacionih sistema u Evropskoj uniji;
7. Postoji potreba za povećanjem svijesti o sajber bezbednosti, preventivnim aktivnostima i razvoju programa veština, e-uprave i kampanja za podizanje znanja i veština u cilju sajber prijetnji;
8. Zaključivanje bilateralnih sporazuma sa proizvođačima informacionih tehnologija u cilju jačanja obuke o sajber bezbednosti za krajnje korisnike i olakšavanja pristupa njihovim proizvodima, uslugama i procesima biće od suštinskog značaja za poboljšanje sajber bezbednosti u Republici Severnoj Makedoniji i šire;
9. Republika Severna Makedonija ima zakonsku regulativu koja određuje ovu pojavu, ali joj je potrebna stalna dopuna kako bi ostala jednaka razvoju novih sajber prijetnji;

[427] Zakon unutrašnjih poslova, Službeni list RSM, 42/14, 116/14,33/15 (2019).

10. Kažnjena politika Republike Severne Makedonije predviđa visoke kazne i zatvorske kazne za počinioce ove vrste zločina, što je pokazatelj da se država zaista bori protiv ove negativne pojave;
11. Republika Severna Makedonija ima odgovarajuće institucionalne kapacitete za rano otkrivanje, poduzimanje zakonskih mera i ublažavanje štete na kritičnoj infrastrukturi uzrokovane kibernetičkim napadima;
12. Reforme u bezbednosno-obaveštajnoj zajednici u Republici Severnoj Makedoniji će pozitivno uticati na nadležne institucije za brz i efikasan odgovor na eliminisanje potencijalne sajber pretnje;
13. Ministarstvo unutrašnjih poslova je ključni faktor u bavljenju kibernetičkim pretnjama i garantuje neophodnu sajber bezbednost za sve građane na celoj teritoriji Republike Severne Makedonije.

KORIŠĆENA LITERATURA:

1. Dončev, A. (2007), Sovremeni bezbednosni sistemi, Aleksandar Dončev, Skopje.
2. Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
3. European Union, Serious and organized crime threat assessment, (2017), Crime in the age of technology, Europol.
4. Gillespie, A. A., (2015), Cybercrime: Key Issues and Debates Florence, Kentucky (USA)
5. Joint communication with the European Parliament and the Council, (2017) European commission, High representative of the union for foreign affairs and security policy, Brussels.
6. Kotovcevski, M., (2011), Nacionalna bezbednost, Filozofski fakultet, Skopje.
7. Lajman.D.M., Poter.V.G., (2009), Organiziran kriminal, Magor, Skopje.
8. Mijalković. V, S., (2011), Nacionalna bezbednost, Kriminalističko policijska akademija, Beograd.
9. Nacionalna strategija za sajber bezbednost na Republika Severna Makedonija (2018) 2018-2022, Vlada na RSM, Skopje.
10. Rajkovčevski, R., (2014), Gradenje bezbednosna politika: slučajot na Republika Makedonija, Fondacija Konrad Adenauer, Kancelarija Skopje.
11. Resilience, Deterrence and Defense (2017): Building strong cyber security in Europe, Tallinn Digital Summit.
12. Spasić, V., Aktuelna pitanja u oblasti sajber kriminala (članak), Bilten sudske prakse Vrhovnog suda Republike Srbije broj. 1/2006, Beograd.
13. Šarkić, N., Prlja, D., Damnjanović, K., Marić, V., Ţivković, V., Vodinelić, V., Mrvić-Petrović, N.: (2011), Pravo informacionih tehnologija, Beograd.

ZAKONSKA AKTA:

1. Krivični zakon Republike Severne Makedonije, Službeni list, 80/99, 4/02, 43/03, 19/04, 81/05, 60/06, 73/06, 7/08, 139/08, 114/09, 51/11, 135/11 , 185/11, 142/12, 166/12, 55/13, 82/13, 14/14, 27/14, 28/14, 115/14, 132/14 (2019).
2. Zakon o klasifikovanim informacijama. Službeni list RSM, 09/04, 113/07, 145/10, 80/12, 41/14, 21/18 (2019).
3. Zakon o praćenju komunikacija, Službeni list Republike Severne Makedonije 71/18 (2019).
4. Zakon o unutrašnjim poslovima, Službeni list Republike Severne Makedonije, 42/14, 116/14, 33/15 (2019).
5. Zakon o policiji, Službeni list Republike Severne Makedonije, 114/06, 06/09, 145/12, 41/14, 33/15 (2019).

6. Zakon o elektronskim komunikacijama, Službeni list Republike Severne Makedonije, 39/14, 188/14, 44/15, 193/15, 11/18, 21/18, (2019).

INTERNET STRANICE:

1. https://www.enisa.europa.eu/about-enisa,
2. https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme,
3. http://www.europarl.europa.eu/doceo/document/A-8-2018-0264_HR.pdf,
4. https://www.europol.europa.eu/socta/2017/introduction.html,
5. https://mvr.gov.mk,