FORENZIČKO RAČUNOVODSTVO, ISTRAŽNE RADNJE, LJUDSKI FAKTOR I PRIMENJENI ALATI

Grupa autora

Prvo izdanje

UNIVERZITET U BEOGRADU
FAKULTET ORGANIZACIONIH NAUKA

Grupa autora
Forenzičko računovodstvo, istražne radnje, ljudski faktor i primenjeni alati
prvo izdanje

Izdavač
Fakultet organizacionih nauka, Beograd, Jove Ilića, br. 154
www.fon.bg.ac.rs

Za izdavača
Dekan, prof. dr Milija Suknović

Uređuje
dr Snežana Knežević, vanredni profesor Fakulteta organizacionih nauka
Univerzitet u Beogradu

Recenzenti
Prof. dr Radojko Lukić, redovni profesor Ekonomskog fakulteta
Univerzitet u Beogradu
Prof. dr Marijana Despotović Zrakić
redovni profesor Fakulteta organizacionih nauka
Univerzitet u Beogradu
Prof. dr Zorica Bodanović, redovni profesor Fakulteta organizacionih nauka,
Univerzitet u Beogradu
dr Cvjetana Cvetković Ivetić, docent, Pravni fakultet
Univerzitet u Novom Sadu
Vladimir Jović, Klinički psiholog, Specijalista medicinske psihologije
Klinika za neurologiju i psihijatriju za decu i omladinu, Beograd

Lektor
Laura Barna

Dizajn
Popović Saša

Tehnička priprema
Snežana Minić

Štampa
„Skripta Internacional“, Beograd

Tiraž
500
Godina izdanja
2021.

ISBN: 978-86-7680-393-4

FORENZIČKO RAČUNOVODSTVO, ISTRAŽNE RADNJE, LJUDSKI FAKTOR I PRIMENJENI ALATI

Autori

Aleksandar Čudan
Aleksandar Đoković
Aleksandar Grgur
Aleksandar Marković
Aleksandar Živković
Aleksandra Mitrović
Andrija Kezunović
Aneta Stojanovska-Stefanova
Boban Ničić
Bojan Cvetković
Bojan Mavrenski
Bosiljka Srebro
Božidar Banović
Dragan Cvetković
Dragan Kecman
Dragan Vasilev
Dragan Živković
Dragoljub Simonović
Dragomir Dimitrijević
Dunja Mekerević
Dušan Marković
Dušan Purić
Duško Šnjegota
Đorđe Mihajlović
Đurđica Trivunović Sajić
Goran Milošević
Hristina Runcheva Tasev
Ivan Marković
Jana Cvijić
Jasmina Paunović
Jasminka Marjanović
Javorka Travica
Jelena Runjić
Jelena Stojanović Alcaraz
Jovan Travica
Lena Đorđević Milutinović
Luka O. Baturan
Marija Milojičić
Marko Milašinović
Marko Špiler
Mia Šešum
Milan Vujić
Milena Apostolovska Stepanoska
Milenko Radonić
Milica Latinović
Miloš Lukić
Miloš Milosavljević
Miloš Milošević
Mina Bulatović
Mirko Kulić
Nikola N. Cvetković
Nikola Vasiljević
Nikola Vuksanović
Nikola Zornić
Olivera Đurić
Slavica Đurić Dakić
Slobodan Antić
Snežana Knežević
Srđan Nikolovski
Stefan Milojević
Stefan Stojanović
Stevan Tomašević
Tamara Vujić
Tatjana Ivanović
Tijana Obradović
Uglješa Mrdić
Veljko Dmitrović
Vesna Bogojević Arsić
Vesna Tornjanski
Vladimir M. Cvetković
Zdravka Petković
Zoran Morić
Žarko Radojičić
Želimir Kešetović
Željko Babić

SADRŽAJ

Prvi deo

PEJZAŽ SAJBER BEZBEDNOSTI I DIGITALNA FORENZIKA: MAKEDONSKA PERSPEKTIVA

dr Hristina Runcheva Tasev
vanredni profesor
Odsek političkih nauka
Pravni fakultet "Iustinianus Primus"
Univerzitet Svetog Ćirila i Metodija u Skoplju
E-mail: h.runchevatasev@pf.ukim.edu.mk

dr Aneta Stojanovska-Stefanova
vanredni profesor
Univerzitet Goce Delčev-Štip
E-mail: aneta.stojanovska@ugd.edu.mk

dr Milena Apostolovska Stepanoska,
vanredni profesor
Odsek političkih nauka
Pravni fakultet "Iustinianus Primus"
Univerzitet Svetog Ćirila i Metodija u Skoplju
E-mail:
m.apostolovskastepanoska@pf.ukim.edu.mk

1. DIGITALNA FORENZIKA - USLOV SINE QUA NON U DIGITALNOM DRUŠTVU

Digitalna forenzika je relativno nova disciplina koja je nastala izazovima nametnutim u digitalnom okruženju. Svaka aktivnost u ovom digitalnom svetu obeležena je digitalnim otiskom koji se verovatno stvara i koji sadrži neku vrstu digitalnih dokaza koji se mogu povratiti.

Sajber incidenti brzo se razvijaju, sve ih je više i sve su ozbiljniji. Kada se dogodi sajber incident, napadnuti subjekat reaguje nizom unapred određenih radnji. Primena digitalne forenzike za pomoć u oporavku i istraživanju materijala na digitalnim medijima i mrežama jedna je od ovih radnji[1].

Forenzika je primena nauke za rešavanje pravnog problema. U forenzici su zakon i nauka zauvek integrisani. Nijedno se ne može primeniti bez odavanja počasti drugome. Najbolji naučni dokazi na svetu su bezvredni ako su neprihvatljivi na sudu[2].

Ali šta čini digitalnu forenziku tako izazovnom u poslednjih nekoliko godina? Počnimo sa definicijama. Postoji mnogo načina za definisanje digitalne forenzike.

Digitalna forenzika je „postupak identifikovanja, očuvanja, analize i iznošenja digitalnih dokaza na način koji je pravno prihvatljiv u bilo kom pravnom postupku (tj. sudu)[3].”

Ken Zatiko, bivši direktor Američke odbrambene laboratorije za računarsku forenziku, daje definiciju orijentisanu ka procesu kada sugeriše da se digitalna forenzika može definisati kao „primena računarske nauke i istražnih postupaka u legalne svrhe koja uključuje analizu digitalnih dokaza nakon odgovarajućeg ovlašćenja za pretragu, lanca pritvora, matematičke validacije, upotrebe potvrđenih alata, ponovljivosti, izveštavanja i moguće stručne prezentacije[4].” U kratkoj belešci o digitalnoj forenzici koja je pripremljena za britanski parlament navodi se da „Ne postoji standardna definicija, ali britanski regulator za forenzičke nauke definiše digitalnu forenziku kao postupak izvlačenja informacija iz medija za skladištenje podataka (npr. uređaja, sistema povezanih sa računarstvom, ...), pretvorenih u upotrebljivu formu, obrađenih i protu-

1 Pregled digitalne forenzike. ISACA, 2015. Dostupno na: https://www.infosecurityeurope.com/__novadocuments/83665?v=635652368156170000. Pristupljeno 1.9.2020.
2 Sammons, John. (2015). Osnove digitalne forenzike- Priručnik za početak rada u digitalnoj forenzici, Second ed. Elsevier. p. 2.
3 Mohay, George M.; Alison Anderson; Byron Collie; Rodney D. McKemmish; Olivier de Vel; Forenzika računara i provale, Artech House, USA, 2003.
4 Zatyko, Ken; “Komentar: Definisanje digitalne forenzike,” Časopis o forenzici, 2 januar 2007,www.forensicmag.com/articles/2007/01/commentary-defining-digital-forensics. Pristupljeno 1.9.2020.

mačenih da bi se dobili podaci za upotrebu u istragama ili dokazi za upotrebu u krivičnom postupku.

Proces digitalne forenzike sastoji se od nekoliko procesa koji se mogu razlikovati tokom istraga. U većini slučajeva uključuju:

- Oporavak – podaci se izdvajaju, što može podrazumevati kopiranje tvrdog diska, preuzimanje podataka sa mobilnog uređaja ili oporavak podataka iz udaljenog sistema. Podaci se zatim obrađuju kako bi ispitivač mogao da radi na njima. To može uključivati dešifrovanje podataka i oporavak datoteka.
- Tumačenje – podaci se analiziraju i tumače, što često uključuje sintezu informacija iz različitih izvora. Ovo može zahtevati značajnu stručnost.
- Prezentacija – saopštavaju se nalazi iz analize; na primer usmeno istražnom timu, kao pisani izveštaj, ili možda eventualno na sudu[5].

Digitalna forenzika je oblast koja se sve više razvija sa mnogo raznolikosti u tehnologijama koje se trajno razvijaju. Od ranih faza digitalne forenzike, kada su prikupljeni dokazi od samostalne mašine do visoko umreženog oblaka i mobilnog okruženja današnjice, stvaraju se mnogi izazovi pred vladama širom sveta.

Brzi tempo tehnoloških promena predstavlja značajan izazov za digitalne forenzičare. Novi hardver, operativni sistemi i aplikacije moraju se proučiti kako bi se otkrilo kako pouzdano pronaći informacije o forenzičkoj vrednosti. Još jedan izazov je velika količina podataka sačuvanim na uređajima, koja je u stalnom porastu tokom godina. Ovo utiče na vreme utrošeno na obradu podataka i pojačan pritisak na forenzičke službe. Odgovor na brzu tehnološku promenu postaje u velikoj meri zavisan od budžeta koji vlade obezbeđuju za sajber bezbednost.

Različiti pristupi sajber sigurnosti preduzeti su kao odgovor na veliki broj pretnji u sajber prostoru.

Ovaj rad će istražiti makedonsko zakonodavstvo koje tretira sajber kriminal i nacionalni pristup jačanju kapaciteta sajber sigurnosti i razvoju digitalne forenzike kao neophodan odgovor na sve veći broj napada koji se dešavaju u sajber prostoru.

5 Ibid.

2. MAKEDONSKI ZAKONODAVNI OKVIR ZA SAJBER BEZBEDNOST

Makedonski sajber ekosistem je još uvek u ranoj fazi. Prema pregledu kapaciteta sajber bezbednosti[6] iz 2018, u nekim vladinim agencijama i vodećim kompanijama, način razmišljanja o sajber bezbednosti počeo je da se razvija.

Način razmišljanja o sajber-bezbednosti sastoji se od vrednosti, stavova i praksi, uključujući navike, pojedinačnih korisnika, stručnjaka i drugih aktera ekosistema sajber-bezbednosti koji povećavaju otpornost korisnika na pretnje njihovoj bezbednosti na mreži.

Međutim, kultura sajber bezbednosti uglavnom nije mnogo napredna i korisnici često nisu svesni rizika povezanih sa upotrebom Interneta. Svest o potrebi zaštite ličnih podataka i upoznavanje sa bezbednosnim problemima u pogledu ličnih podataka je generalno niska.[7]

Makedonski pravni sistem nema sveobuhvatan zakon koji se bavi isključivo sajber bezbednošću[8].

Ključni međunarodni izvor koji daje smernice za tretman sajber kriminala u makedonskom zakonodavstvu je Budimpeštanska konvencija o sajber kriminalu[9] koju je usvojilo Savet Evrope ratifikovan u makedonskom parlamentu 2004. godine. Dodatni protokol uz Konvenciju o sajber kriminalu[10] u vezi sa kriminalizacijom dela rasističke i ksenofobične prirode počinjenih putem računarskih sistema ratifikovana je u novembru 2005. godine.

Umesto toga, nekoliko pravnih dokumenata dotiče se pojedinih pitanja vezanih za sajber sigurnost – Zakon o ličnim podacima, Zakon o elektronskoj trgovini, Zakon o elektronskim komunikacijama, Zakon o presretanju komunikacija, Zakon o slobodnom pristupu javnim informacijama, Zakon o Podacima u elektronskom obliku i elektronski potpis. Takođe, izmene i dopune Zakona o krivičnom postupku usvojene 2013. godine posebno se bave sajber

6 BJR Makedonija 2018. Dostupno na: https://ssrn.com/abstract=3658462, Pristupljeno: 15.9.2020.
7 Ibid.
8 Diplo Foundation (2016) Sajber bezbednost na zapadnom Balkanu: Jazovi u politikama i mogućnosti saradnje. https://www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20Western%20Balkans.pdf, Pristupljeno 15.9.2020.
9 Savet Evrope (2006) Dodatni protokol uz Konvenciju o sajbern kriminalu, koji se tiče kriminalizacije dela rasističke i ksenofobične prirode počinjenih putem računarskih sistema. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189, Pristupljeno: 15.9.2020.
10 Savet Evrope (2001) Konvencija o sajber kriminalu, 23 novembar 2001. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, Pristupljeno: 15.9.2020.

kriminalom i zločinima počinjenim uz upotrebu računara, kao i prikupljanjem digitalnih dokaza od strane organa za sprovođenje zakona.[11]

U julu 2018. godine razvijena je i usvojena Nacionalna strategija sajber bezbednosti,[12] a kasnije 2018. poboljšana je usvajanjem Akcionog plana[13] za sprovođenje Strategije.

Iako ne postoji jedinstveni sveobuhvatni pravni okvir koji se eksplicitno bavi sajber-sigurnošću, postoji nekoliko zakona koji pokrivaju osnove sajber bezbednosti u zemlji.

Najvažniji izvor zakona o sajber kriminalu u zemlji je Krivični zakonik sa odredbama u deset njegovih članova; bavi se sajber kriminalom kao što su zloupotreba ličnih podataka, autorska prava i piraterija, proizvodnja i distribucija dečije pornografije, računarski virusi, upadi u računarske sisteme, računarska prevara i kompjuterski falsifikat.

Takođe, amandmani usvojeni 2013. godine odnose se na prikupljanje digitalnih dokaza od strane organa za sprovođenje zakona. Nakon usvajanja Budimpeštanske konvencije 2004. godine, pristup se promenio 2011. godine, sa manjim fokusiranjem na istrage o sajber kriminalu a više na prikupljanje elektronskih dokaza, uopšte. MUP podržava sve istrage povezane sa elektronskim dokazima.[14] Izgradnja kapaciteta MUP-a za sprovođenje i podršku svih vrsta istraga u vezi sa sajber kriminalom trebalo bi da ostane jedan od najviših prioriteta u narednim godinama.

Takođe, ne postoji konkretno zakonodavstvo o ljudskim pravima na mreži, ali država je potpisnica međunarodnih instrumenata o ljudskim pravima, poput Evropske konvencije o ljudskim pravima i Ženevske konvencije Ujedinjenih nacija o statusu izbeglica i Konvencije protiv mučenja.

Sveobuhvatno zakonodavstvo o zaštiti dece na mreži usvojeno je i primenjuje se prema članovima 193 i 193a Krivičnog zakonika.[15] Poziva se na član 9 Budimpeštanske konvencije koji reguliše distribuciju materijala za zlostavljanje dece na mreži. Od 2010. godine, Krivičnom zakonu dodate su nove

11 Diplo Foundation (2016) Sajber bezbednost na zapadnom Balkanu: Jazovi u politikama i mogućnosti saradnje. https://www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20Western%20Balkans.pdf., Accessed on 15.9.2020.

12 Nacionalna strategija sajber bezbednosti 2018-2022, MIOA, Pristupljeno: https://mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/cyber_security_strategy_macedonia_2018-2022_-_eng.pdf, Accessed on 15.9.2020.

13 Nacionalni akcioni plan za sajber bezbednost 2018-2022, MIOA. Pristupljeno: https://mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/ap_cybersec_v1.13_eng.pdf, Pristupljeno: 15.9.2020.

14 Ibid.

15 Zakon o krivičnom zakoniku,Službeni glasnik .37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 50/2006, 60/2006, 73/2006, 87/2007, 7/2008, 139/2008, 114/2009, 51/2011, 51/2011, 135/2011, 185/2011, 142/2012, 143/2012, 166/2012, 55/2013, 82/2013.

izmene koje uključuju zakonske odredbe o dečjoj pornografiji na mreži i seksualne nege na mreži.

Pored toga, nakon ratifikacije Budimpeštanske konvencije 2004. godine, Krivični zakonik je promenjen kako bi ispunio obaveze u vezi sa zaštitom potrošača i intelektualnom svojinom na mreži. 2016. godine nove zakonske odredbe dodate su Zakonu o zaštiti potrošača (2004.) kako bi se uskladile sa zakonodavstvom o zaštiti potrošača u EU.

Ministarstvo unutrašnjih poslova (MUP) bilo je uključeno u izradu zakonskih odredbi Krivičnog zakonika i zaduženo je za njegovu primenu. Na nacionalnom nivou, makedonska carinarnica i Koordinaciono telo za intelektualno vlasništvo su odgovorne institucije koje regulišu intelektualnu svojinu proizvoda i usluga na mreži.

Odredbe Budimpeštanske konvencije prenete su u Krivični zakonik i Zakon o krivičnom postupku, koji se smatraju najvažnijim delovima zakona koji se bave sajber kriminalom[16].

3. INSTITUCIONALNI KAPACITETI

U pogledu institucionalnih kapaciteta za bavljenje pitanjima sajber kriminala, Jedinica za sajber kriminal koja se nalazi u okviru Odeljenja za suzbijanje organizovanog i teškog kriminala i Forenzičko odeljenje Ministarstva unutrašnjih poslova spojila su se u jedinstveno Odeljenje za sajber kriminal i digitalnu forenziku, čineći tako efikasnije i efektivnije istražne jedinice[17].

Odeljenje za sajber kriminal i digitalnu forenziku pri MUP-u jedina je jedinica u zemlji koja može da istražuje slučajeve sajber kriminala. Digitalni forenzičari se fokusiraju na forenzičke istrage i organizovani su u dva pododseka/specijalizacije: računarska forenzika i mobilna forenzika.

Što se tiče kapaciteta, Odeljenje za sajber kriminal i digitalnu forenziku pri MUP-u ima 22 službenika koji su sertifikovani profesionalci; dobili su sledeća zvanja: ovlašćeni stručnjak za bezbednost informacionih sistema (CISSP), ovlašćeni etički haker (CEH) koje je obezbedio Savet EZ i sertifikat ovlašćenog forenzičkog računarskog ispitivača (CFCE).[18.]

Podaci koji se odnose na digitalnu opremu zaplenjenu na mestu zločina

16 Pregled kapaciteta za sajber bezbednost BJR Makedonija 2018. Dostupno na: https://ssrn.com/abstract=3658462. Accessed on 15.9.2020.
17 Diplo Foundation (2016) Sajber bezbednost na zapadnom Balkanu: Jazovi u politikama i mogućnosti saradnje https://www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20Western%20Balkans.pdf, Pristupljeno 15.9.2020.
18 Pregled kapaciteta za sajber bezbednost BJR Makedonija 2018. Dostupno na: https://ssrn.com/abstract=3658462. Pristupljeno 15.9.2020.

ispituju se u ovoj jedinici. Svaki inspektor sa terena, zajedno sa nalogom javnog tužioca ili sudije, može doneti digitalni uređaj. Nalog sadrži informacije o tome ko je vlasnik opreme, koji su dokazi povezani sa njom, šta treba pronaći, lozinke, šifrovane podatke. Izveštaji digitalnih forenzičara iznose se na sud i prihvataju kao dokaz[19].

Jedinica se takođe bavi zahtevima za sadržajem i / ili podacima o saobraćaju. Takve naredbe šalju se od javnog tužioca dobavljaču usluga i zaplenjuju se svi podaci - i podaci o sadržaju i saobraćaju od strane stručnjaka jedinice. Kada se informacije zatraže od banke, administrator dostavlja evidencije policiji - spakovane i heširane (Heš funkcije se prvenstveno koriste za generisanje fiksne dužine izlaznih podataka Prim.prev. Heš čuvaju banka i organi reda.[20]

Prema Zakonu o krivičnom postupku, MUP sarađuje sa tužiocem koji ima glavnu ulogu u istrazi o sajber kriminalu. Sprovođenje zakona deluje samo kao posrednik za prikupljanje elektronskih dokaza tokom istrage i na suđenju. Nažalost, zbog nedostatka kapaciteta, MUP nije u mogućnosti da pruži podršku svim tužiocima u zemlji u vezi sa prikupljanjem digitalnih dokaza sa elektronskih uređaja. Oni rade sa samo dve forenzičke laboratorije (jedna za mobilne uređaje, a druga za računarsku forenziku).

Postoji potreba za jačanjem kapaciteta u različitim institucijama, poput Kancelarije finansijske policije i Ministarstva finansija, gde trenutno radi samo jedan istražitelj[21]. Ovaj proces bi trebalo da bude praćen decentralizacijom kapaciteta digitalne forenzike između nekoliko institucija. Istraga slučajeva finansijskog sajber kriminala trebalo bi da bude poverena Finansijskoj policiji kao odgovarajućem telu za istragu, uz podršku Uprave prihoda.

Institucionalni kapacitet sudija i tužilaca za bavljenje slučajevima sajber kriminala i slučajevima koji uključuju digitalne dokaze je takođe ograničen. To je zbog budžetskih ograničenja i nedovoljnog nivoa potrebne tehničke opreme. U zemlji ne postoje posebni sudovi za postupanje u slučajevima sajber kriminala. Sudije i tužioci nemaju specijalnu obuku o sajber kriminalu niti o digitalnim dokazima.

Implementacijom Akcionog plana Strategije za sajber kriminal iz 2017. godine, MUP razvija MC4 (Makedonska platforma za sajber

19 Izveštaj Savetodavna misija i radionica o mrežnim prevarama i drugim mehanizmima izveštavanja o sajbern kriminalu 20. - 21. februara 2017. godine, Skoplje „Bivša jugoslovenska republika Makedonija“, obezbeđeno u okviru projekta iPROCEEDS, 2017., SE i EU. Dostupno: https://rm.coe.int/3156-26-iproceeds-report-reporting-mechanisms-mk/16807be381.Pristupljeno 15.9.2020.
20 Ibid.
21 Pregled kapaciteta za sajber bezbednost BJR Makedonija 2018. Dostupno na: https://ssrn.com/abstract=3658462. Accessed on 15.9.2020.

kriminal / Centar za žalbe) kako bi građanima pružao informacije i novosti o pitanjima sajber kriminala, kao što su vesti o načinu rada prestupnika na Internetu, i sredstva za anonimno prijavljivanje bilo koje aktivnosti povezane sa sajber kriminalom (npr. sumnjive aktivnosti na Darknetu ili forumima)[22].

Uprkos naporima, zbog ograničenih institucionalnih kapaciteta i nedostatka kvalifikovanog osoblja još uvek ne dozvoljavaju napredne istražne postupke u vezi sa ozbiljnim slučajevima sajber kriminala.

Izveštaji stručnjaka ukazuju na da je neophodna dodatna obuka za one koji reaguju prvi put sa fokusom na to kako da oduzmu opremu na mestu zločina.

Takođe postoji potreba za obukom policajaca o prirodi i zahtevima digitalnih dokaza. Treba razviti sposobnost forenzike podataka uživo. Takođe, potrebna je dodatna obuka o istragama kripto valuta, jer nema dovoljno iskustva u ovoj oblasti[23].

U okviru institucionalnih kapaciteta u vezi sa incidentima sajber bezbednosti, osnovan je Makedonski tim za reagovanje na računarske incidente (MKD-CIRT). Služi kao nacionalno koordinaciono telo za izveštavanje i upravljanje incidentima sajber bezbednosti za organe vlasti i institucije javnog sektora. U 2015. godini MKD-CIRT je uspostavljen u okviru Agencije za elektronske komunikacije kao „zvanična nacionalna tačka za kontakt i koordinaciju u rešavanju bezbednosnih incidenata u mrežama i informacionim sistemima" prema Zakonu o elektronskim komunikacijama.[24]

22 Ibid.

23 Izveštaj Savetodavna misija i radionica o mrežnim prevarama i drugim mehanizmima za izveštavanje o sajber kriminalu 20. - 21. februara 2017., Skoplje „Bivša jugoslovenska republika Makedonija", obezbeđeno u okviru projekta iPROCEEDS, 2017., SE i EU. Dostupno na: https://rm.coe.int/3156-26-iproceeds-report-reporting-mechanisms-mk/16807be381. Pristupljeno 15.9.2020.

24 Agencija za elektronske komunikacije. MKD-CIRT. https://mkd-cirt.mk/?lang=en, Pristupljeno 15.9.2020.

4. CILJEVI I OČEKIVANJA NACIONALNE STRATEGIJE SAJBER BEZBEDNOSTI

Politička i ekonomska nestabilnost na zapadnom Balkanu stvara ranjiv prostor za brojne pretnje i izazove. Sajber prostor nije izuzetak, sa povećanim brojem sajber napada, koji su ovu pretnju stavili na vrh nacionalnih prioriteta kojima se treba pozabaviti. Jačanje makedonskih kapaciteta za sajber bezbednost takođe je bilo na dnevnom redu vlade u poslednjoj deceniji, pored složenog političkog i socijalno-ekonomskog pejzaža zemlje. Transformativni proces podizanja svesti o rizicima i mogućnostima sajber bezbednosti postao je regionalni trend i praćen je procenama sajber bezbednosti, razvojem novih operativnih i strateških planova, uspostavljanjem organa i entiteta za sajber bezbednost, razvojem obrazovnih programa kako bi se udovoljilo potražnji stručnjaka za sajber bezbednost na sadašnjem i budućem tržištu rada itd.

Predeo sajber bezbednosti je izazov jer se trajno menja, tako da strateški dokumenti moraju biti trajno revidirani i nadograđivani. Brze i efikasne institucionalne reakcije zahtevaju izgradnju kapaciteta za sajber bezbednost, što bi trebalo da ostane kao dugoročni cilj. Zahteva značajno korišćenje budžetskih sredstava, a vrlo često budžetska ograničenja predstavljaju prepreku za efikasnu primenu usvojenih strateških dokumenata. Sticanje finansijskih, ljudskih i tehnoloških resursa često se smatra nepotrebnim ulaganjem. Nacionalni pristup trebalo bi da se zasniva na pristupu više zainteresovanih strana, domaćih i međunarodnih, uključujući civilno društvo i akademsku zajednicu.

Izazovi u sajber bezbednosti moraju se rešiti dugoročnom strategijom za podizanje svesti i bolju sajber kulturu u različitim segmentima društva. Regionalna saradnja u ovom kontekstu može olakšati pristup uspostavljanju sigurnijeg sajber prostora za zemlje koje se suočavaju sa sličnim pretnjama po pitanju sajber bezbednosti. Sprovođenje zajedničkih kampanja za podizanje svesti o sajber bezbednosti, zajedno sa javnim angažovanjem različitih zainteresovanih strana, edukacijom i razmenom dobrih praksi, imalo bi značajniji uticaj ako bi se sprovodilo na regionalnom nivou.

Makedonska nacionalna strategija sajber sigurnosti zasniva se na pet ključnih ciljeva:[25]

1. Sajber otpornost: postojanje nacionalne sajber otporne IKT infrastrukture i identifikovanje i primena adekvatnih rešenja za zaštitu nacionalnih interesa.
2. Sajber kapacitet i kultura sajber bezbednosti: Javni, privatni sektor i makedonsko društvo da sveobuhvatno razumeju sajber pretnje i da imaju potrebne kapacitete da se zaštite.
3. Borba protiv sajber kriminala: Jačati kapacitete zemlje za prevenciju, istraživanje i adekvatan odgovor na sajber kriminal.
4. Sajber odbrana da ojača nacionalne kapacitete kako bi mogao da zaštiti nacionalne interese i smanji trenutne i buduće rizike u sajber prostoru.
5. Saradnja i razmena informacija: zaštititi sajber prostor zemlje saradnjom i razmenom informacija na nacionalnom i međunarodnom nivou, kako bi se omogućio otvoren, slobodan, stabilan i bezbedan sajber prostor.

Ciljeve bi trebalo postići sprovođenjem brojnih aktivnosti, a prioritet se daje pripremi zakona za informacionu bezbednost (primena Direktive EU NIS 2016/1149) koji je u zakonodavnoj proceduri od 2019. godine. Prioritet je dat i primeni akcionog plana Nacionalne strategije sajber bezbednosti, koji uključuje uspostavljanje Regionalnog centra za obuku i istraživanje sajber bezbednosti, poboljšanu međunarodnu saradnju, izgradnju institucionalnih kapaciteta i obrazovanje i podizanje svesti o sajber bezbednosti. Nacionalno telo za IKT i sajber bezbednost sa operativnim kapacitetima za sajber bezbednost osnovano je 2019. godine, kao jedan od prioriteta Strategije i Akcionog plana.

Uzimajući sve ovo u obzir, makedonski pejzaž sajber bezbednosti pokazuje ozbiljnu posvećenost i sveobuhvatno razumevanje sajber pretnji. Kulturu sajber bezbednosti trebalo bi poboljšati i ojačati regionalnu saradnju u rešavanju sajber pretnji koje mogu pružiti otvoren, slobodan, stabilan i siguran sajber prostor.

25 National Cyber Security Strategy 2018-2022, MIOA, Available at https://mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/cyber_security_strategy_macedonia_2018-2022_-_eng.pdf, Accessed on 15.9.2020.

LITERATURA

Agency for Electronic Communications. *MKD-CIRT*.Available at: https://mkd-cirt.mk/?lang=en. Accessed on 20.9.2020.

Council of Europe (2001) *Convention on Cybercrime,* 23 November 2001. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, Accessed on 15.9.2020.

Council of Europe (2006) *Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems*, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189, Accessed on 15.9.2020.

Cybersecurity Capacity Review FYR Macedonia 2018. Available at: https://ssrn.com/abstract=3658462. Accessed on 15.9.2020.

DiploFoundation (2016*) Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities*, https://www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20Western%20Balkans.pdf, Accessed on 15.9.2020.

DiploFoundation (2016) *Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities*. https://www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20Western%20Balkans.pdf, Accessed on 15.9.2020.

Law on Criminal Code, Official Gazette No .37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 50/2006, 60/2006, 73/2006, 87/2007, 7/2008, 139/2008, 114/2009, 51/2011, 51/2011, 135/2011, 185/2011, 142/2012, 143/2012, 166/2012, 55/2013, 82/2013.

Mohay, George M.; Alison Anderson; Byron Collie; Rodney D. McKemmish; Olivier de Vel; *Computer and Intrusion Forensics,* Artech House, USA, 2003.

National Cyber Security Action Plan 2018-2022, MIOA. Available at: https://mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/ap_cybersec_v1.13_eng.pdf, Accessed on 15.9.2020.

National Cyber Security Strategy 2018-2022, MIOA, Available at https://mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/cyber_security_strategy_macedonia_2018-2022_-_eng.pdf.

Overview of Digital Forensics. ISACA (2015) Available at https://www.infosecurityeurope.com/__novadocuments/83665?v=635652368156170000. Accessed on 1.9.2020.

Parliamentary Office of Science and Technology, *Digital Forensics and Crime,* Post Note 520 (March 2016). Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwing5fr0JnsAhVClosKHaxKDdwQFjABegQIAxAC&url=http%3A%2F%2Fresearchbriefings.files.parliament.uk%2Fdocuments%2FPOST-PN-0520%2FPOST-PN-0520.pd-

f&usg=AOvVaw1BmLjrNdtV1pAP-tN-XWpM. Accessed on: 1.9.2020.

Report Advisory mission and workshop on online fraud and other cybercrime reporting mechanisms 20 - 21 February 2017, Skopje "The former Yugoslav Republic of Macedonia", Provided under the iPROCEEDS project, 2017, CoE and EU. Available at: https://rm.coe.int/3156-26-iproceeds-report-reporting-mechanisms-mk/16807be381. Accessed on 15.9.2020.

Sammons, John. (2015). *The Basics of Digital Forensics- The Primer for Getting Started in Digital Forensics*, Second ed. Elsevier. p. 2.

UK Forensic Science Regulator *Newsletter* No. 26 (2015). Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/470526/FSR_Newsletter_26__October_2015.pdf., Accessed on 01.9.2020.

Zatyko, Ken; "Commentary: Defining Digital Forensics," *Forensic Magazine,* 2 January 2007, www.forensicmag.com/articles/2007/01/commentary-defining-digital-forensics. Accessed on 1.9.2020.