PISMENOST U OBLASTI SAJBER BEZBJEDNOSTI U CRNOJ GORI
CYBER SECURITY AWARENESS IN MONTENEGRO

Igor Ognjanović, Ramo Šendelj, *Univerzitet Donja Gorica, Crna Gora*
Ivana Ognjanović, *Univerzitet Mediteran, Crna Gora*

Sadržaj: *Ostati zaštićen od sajber sigurnosnih prijetnji zahtijeva da svi korisnici budu svjesni prijetnji i svojim aktivnostima na Internetu sami primijene sigurnosne mjere i prakse u skladu sa postojećim standardima. U ovom radu se prikazuje analiza trenutnog nivoa pismenosti u oblasti sajber bezbjednosti u Crnoj Gori, kao i poređenje sa zemljama iz EU približno male populacije (Kipar, Malta i Luksemburg). Predstavljeni rezultati su osnov za dalje kreiranje okvira za unapređenje obrazovnog sistema (uključujući sve nivoe formalnog, kao i neformalno obrazovanje) koje je neophdono implementirati u cilju povećanja nacionalnih kapaciteta u borbi sa sajber prijetnjama i izazovima.*

Abstract: *Staying protected from cyber security threats requires that all users are aware of the threat and its activities on the Internet alone implement security measures and practices in accordance with existing standards. This paper deals with the current level of literacy in the field of cyber security in Europe, as well as the comparison with the countries of the EU about small populations (Cyprus, Malta and Luxembourg). The presented results are the basis for further creating a framework for improving the education system (including all levels of formal and non-formal education) that is neophdono implemented in order to increase national capacity in the fight against cyber threats and challenges.*

1. UVOD

Internet omogućava korisnicima prikupljanje, objavljivanje, obradu i prenos velike količine podataka, uključujući finansijske transakcijskih, lične i osjetljive poslovne podatke itd. Što se više pojedinci i kompanije oslanjaju na takve mogućnosti, sajber napadi postaju sve učestalije i sve više kruže internet prostorom.

Ostati zaštićen od sajber sigurnosnih prijetnji zahtijeva da svi korisnici budu svjesni prijetnji i svojim aktivnostima na Internetu sami primijene sigurnosne mjere i prakse u skladu sa postojećim standardima [1,3]. Crna Gora je kao zemlja u razvoju uspostavila osnove pravnog okvira u oblasti sajber bezbjednosti [5,6] i prepoznala neophodnost [4] za daljim razvojem obrazovnog sistema, uključujući sve nivoe formalnog obrazovanja, povećanje nivoa svijesti građana, edukaciju zaposlenih u javnim i privatnom sektoru, itd.

U ovom radu se prikazuje analiza trenutnog nivoa pismenosti u oblasti sajber bezbjednosti, kao i poređenje sa zemljama iz EU približno male populacije kao i Crna Gora (Kipar, Malta i Luksemburg). Istraživanje je zasnovano na zvaničnim podacima EUROSTAT[1]-a, na osnovu kojih je kreiran model za unapređenje obrazovnog sistema u oblasti sajber bezbjednosti u Crnoj Gori, u okviru Tempus projekta '*Unapređenje obrazovnog sistema u oblasti sajber bezbjednosti u Crnoj Gori- ECESM*', br. 544088-TEMPUS-1-2013-1-SI-TEMPUS-JPHES.

Rad je strukturiran na sljedeći način: poglavlje 2 daje osnovne koncepte sajber bezbjednosti, poglavlje 3 predstavlja odgovarajuće podatke iz EUROSTAT statistike relevantne za procjenu sajber pismenosti na nacionalnom nivou u Crnoj Gori. Poglavlje 4 je fokusirano na poredbenoj analizi za zemljama EU, dok poglavlje 5 zaključuje rad sa okvirom za unapređenje i dalji razvoj u okviru sistema edukacije u Crnoj Gori u oblasti sajber bezbjednosti.

2. OSNOVNI KONCEPTI SAJBER BEZBJEDNOSTI

Pojam *sajber-prostor* može se najbolje shvatiti kao metafora koja se odnosi na virtualni svijet informacionaih sistema. Pojam "prostor" u *sajber-prostoru* se može smatrati više srodnim apstraktnom matematičkom smislu te riječi, a ne fizičkom terenu. Gerenalno, pojam *sajber-prostor* se koristi za opisivanje nefizičkog prostora koji se sastoji od računarskih sistema i informacionih sistema kojima se može pristupiti putem računarskih mreža [7].

Pojam *sajber-bezbjednost* je u opštoj upotrebi od 2000.god i odnosi se na povjerljivost, integritet i dostupnost informacija u sajber prostoru [1]. U cilju uspostavljanja sveobuhvatnog okvira koji je sposoban da odgovori na savremene izazove u sajber prostoru, neophodno je analizirati sigurnosne domene predstavljene na slici 1[8] .

Državni nivo (engl. *Govermental Domain*). Unutar vlade neke države, nije neobično da postoji i do desetak različitih agencija i tijela za nacionalnu sajber sigurnost u različitim oblicima, uključujući i vojsku, pravosuđe, ekonomiju i privredu, infrastrukturu, telekomunikacija, itd. S obzriom da svaka država mora da upsostavi jasne i snažne mjere zaštite svoje kritične infrastrukture, navedena organizacija na nivou vlade jedne države zahtijeva dodatne mjere koordinacije i uspostavljanja koherentnosti u akcijama.

Međunardoni nivo (engl. *International Domain*). Strategija svake države u sajber bezbjednosti podrazmijeva i obuhvata međunarodnu dimenziju, upravo zbog globalnosti Interneta i infromacija koje se prenose. Ovime se dobijaju

[1] http://ec.europa.eu/eurostat

sljedeći nivoi i aspekti u analizi međunarodnog nivoa sajber bezbjednosti: od međunarodno obavezujućih ugovora(npr. *Council of Europe Cybercrime Convention* [9]), do politički obavezujućih ugovora (npr. *Confidence Building Measures in Cyberspace* [10]), kao i nevladinih sporazuma među tehničkim sertifikacionim tijelima (npr. članstvo u FIRST[2] ili sličnim tijelima).

Nacionalni nivo (engl. *National Domain*). Osim aktivnosti vlade i vladinih institucija, neophodno je uključiti sve ostale učesnike: provajdere telekomunikacionih usluga, pivatni sektor, civilno društvo itd. Ovakav pristup uključenja svih činilaca na nacionalnom nivou je opšte prihvaćen i poznat pod nazivom *Nacija kao jedno* (engl. *Whole of Nation*), a vlade mnogih država se odlučuju na preuzimanje mjera za podsticanje saradnje među svim akterima na nacionalnom nivou (osim direktne benefiti u povećanju nivoa zaštite, daje se mogućnost i komercijalizacije itd).

Unutar nacioanlnog nivoa sajber bezbjednosti mogu se identifikovati sljedeći podnivoi:

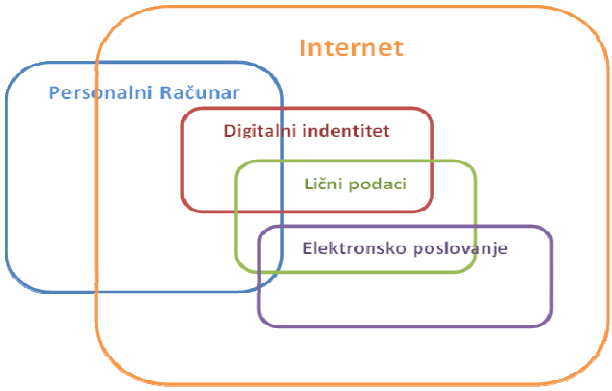
Nivo odbrane (engl. *Defence*). Odbrana na nacionalnom nivou obuhvata širok opseg aktivnosti u cilju zaštite individualno stanovnika, kao i zaštite kompanija i korporacija. Takođe, poseban aspekat odbrane se donosi na aktivnosti u zaštiti od sajber ratova koji su obično u nadležnosti vojske, pa se u nekim metodologijama ovaj nivo posebno odvaja pod nazivom **Vojni aspekat sajber odbrane** (engl. *Military Cyber*).

Kritična informatička infrastruktura (engl. *Critical Information Infrastructure- CIIP*). Danas se u brojnim teorijskim analizama "kritična informatička infrastruktura" najčešće određuje kao skup informatičkih sistema i sredstava koji su ključni za normalno funkcionisanje države.

Stanovništvo (engl. *Citizens*). Stanovništvo je jedan od ključnih faktora u uspostavljanju nivoa sajber zaštite: svaki pojedinac svojim aktivnostima u svakodnevnoj upotrebi Interneta treba da doprinese povećanju nivoa lične sajber bezbjednosti, a profesionalci i pojedinci sa odgovarajućim funkcijama i odgovornostima direktno doprinose nivo opšte nacionalne sajber bezbjednosti.

Slika 1. Odnos između sajber bezbjednosti i ostalih sigurnosnih domena [8]

Predstavljeni domeni sajber bezbjednosti nedvosmisleno ističu značaj ljudskih faktora na procjenu trenutnog nivoa sajber bezbjednosti, kao i definisanje daljih mjera na institucionalnom i nacionalnom nivou. U sljedećem poglavlju se predstavljaju podaci koji ukazuju na nivo pismenosti u oblasti sajber bezbjednosti, gdje se pojam pismenosti u ovom domenu odnosi na procjenu osnovnih znanja i vještina s tri stanovišta [11]: (i) učestalosti upotrebe računara i Interneta, (ii) znanja i vještine pojedinaca u radu na računaru i upotrebi Interneta i (iii) vrsta aktivnosti na Internetu. Navedene procjene će omogućiti kreiranje osnovnih pokazatelja na nacionalnom nivou, u skladu sa segmentacijom znanja i vještina u oblasti sajber bezbjednosti prikazanih na Slici 2.



Slika 2. Segmentacija znanja i vještina korisnika Interneta[11]

3. SAJBER PISMENOST U CRNOJ GORI

Kada se govori o sajber pismenosti na nacionalnom nivou, neophodno je identifikovati odgovarajuće grupe korisnika IT usluga i njima tipične onlajn aktivnosti; na osnovu čega se dalje vrši procjena potrebnog nivoa edukacije i vještina.

Kategorije korisnika su identifikovane isključivo na osnovu starosne dobi, oslanjajući se na očekivanjima da oni dijele iste navike i potrebe u pogledu IT usluga i servisa. Drugim riječima, grupe korisnika se identifikuju sa stanovišta [2, 11]: (i) različite infrastrukture koju koriste pa ju je stoga potrebno i zaštiti, (ii) različitih radnji koje obavljaju, i (iii) različite percepcije i znanje o onlajn sigurnosnim pitanjima. Identifikovane kategorije i uobičajene IT aktivnosti su predstavljene u Tabeli 1.

Kako bi se shvatiti složenost sajber prostora Crne Gore, važno je analizirati statističke podatke o upotrebi IT servisa i usluga u Crnoj Gori. Istraživanje koje je sprovedeno od strane Zavoda za statistiku Crne Gore[3] odnosi se na upotrebu IT-a od strane pojedinaca i kompanija u Crnoj Gori. Istraživanje je sprovedeno po Eurostat metodologiji i obuhvata domaćinstva s najmanje jednim članom dobi između 16 i 74 godina, pojedince iste starosne dobi, kao i kompanije s 10 i više zaposlenih.

Rezultati kompetnog istraživanja su dostupni u [12], dok se u nastavku izdvajaju sljedeći:

- 53.7% domaćinstava ima računar
- 63.6% domaćinstava ima pristup Internetu
- 99.2% domaćinstava ima TV pristup
- 93.6% domaćinstava posjeduje mobilni telefon

[2] Forum for Incident Response and Security Teams: https://www.first.org/

[3] Zavod za statistiku Crne Gore: http://www.monstat.org/

Od svih domaćinstava koji imaju pristup Internetu, njih 75.1% koristi računar, 57.6% koristi lap top, a 38.5% koristi mobilni telefon za pristup Internetu.

Tabela 1. Grupe korisnika i IT aktivnosti (V-visok nivo, S-srednji nivo, N-niski nivo)

Iznad 75 god	64-75 god	55-64 god	46-54 god	34-45 god	18-33 god	Ispod 18 god	IT aktivnosti
N	N	N	S	S-V	S-V	N	**e-mail**
N	N	S	S	V	V	V	**Socijalne mreže**
N	N	S	S	V	S	N	**Informacije o zdravlju**
N	N	S	S	S	V	V	**Multimedijalni sadržaji**
S	S	S	V	V	V	S	**Novosti i blogovi**
N	N	S	S	V	V	V	**Instant poruke**
N	N	V-S	V	V	V	S	**Onlajn kupovina**
N	N	N	V	V	V	S	**Rezervacija putovanja**
N	N	N	N	S	V	V	**Onlajn igre**
N	N	S	S	V	N-S	-	**e-bankarstvo**

Domaćinstva koja nemaju pristup Internetu su dali različite razloge koji su predstavljeni u Tabeli 2. Važno je primijetiti da je čak 33.2% navelo da je nedostatak osnova IT pismenosti razlog za nepostojanje pristupa Internetu u domaćinstvu.

Tabela 2. Razlozi za odsustvo pristupa Internetu u domaćinstvu

Razlog	% odgovora	Razlog	% odgovora
Ne želim pristup Internetu	36,8	Fizička nemogućnost	9,5
Nemam osnove IT pismenosti	33,2	Imam Internet pristup na nekom drugom mjestu	7,5
Pristup Internetu je previše skup	29,9	Interneta konekcija nije dostupna na datom području	5,8
Oprema je previše skupa	27,8	Ostalo	19,6

Podaci o radu na računaru i upotrebi Interneta od starne pojedinaca sumarno pokazuju da:
- 64.5% ispitanika je koristilo računar u poslednjih 3 mjeseca
- 30.6% ispitanika nikada nije koristilo računar
- 63.9% korsnika je korsitilo Internet u poslednjih 3 mjeseca.

Detalji o vrstama aktivnosti na Internetu su prikazani u Tabelama 3 i 4 (kolona koja se odnosi na Crnu Goru).
S druge strane, upotreba Interneta u poslovnom sektoru se karakteriše sledećim podacima:
- 98.1% kompanija u Crnoj Gori koristi računare
- 93.9% kompanija koristi Internet
- 68% kompanija ima svoj veb sajt
- 57% kompanija koristi kompanijski email
- 47.8% koristi neki od servisa na *cloud*-u

S obzirom da su u prethodnih par godina mnoge aktivnosti i projekti bili usmjereni na jačanje IT pismenosti u Crnoj Gori, može se uočiti da je ostvaren određeni napredak u odnosu na prethodnu deceniju [11], ali da ipak predstavljeni podaci nijesu na EU nivou. Takođe se može uočiti da ne postoji usaglašenost između upotrebe Interneta u domaćinstvima i poslovnom sektoru, pa se nameće pitanje o nivou znanja i vještina zaposlenih koji iz nekog razloga nemaju računar i/ili Internet kod kuće, a isti koriste u kompanijama.
Kakogod, IT pismenost je samo osnovni preduslov za učešće u sajber prostoru, a u sljedećem poglavlju se navodi analiza nivoa znanja i vještina u ovoj oblasti.

4. POREDBENA ANALIZA SA EU STANDARDIMA I PRAKSOM

U cilju predstavljanja komparativne analize osnovnih indikatora o znanju i vještinama upotrebe računara i Interneta, korišćeni su rezultati evropske statistike EU28 iz 2012.god, kao i sledeće tri države koje su približno male populacije kao i Crna Gora (populacija: 620.029): Kipar (populacija: 858.000), Luksemburg (populacija: 549.680), Malta (populacija: 425.384).

Tabela 3. Pokazatelji znanja/vještina rada na računaru

	EU28 (2012)	Crna Gora	Kipar	Luksemburg	Malta
Kopiranje fajla/foldera	62%	78.70%	55%	78%	56%
Prenos podataka sa računara na eksterni uređaj	52%	51.90%	45%	80%	47%
Instalacija/konekcija na drugi uređaj	42%	42.70%	33%	60%	32%
Kompresija fajla	35%	32.60%	30%	55%	36%
Rad sa programima za kalkulacije	41%	22.90%	39%	66%	41%
Kreiranje prezentacija pomoću odgovarajućeg softvera	31%	18.90%	31%	51%	33%
Instalacija/unapređenje postojećeg operativnog sistema	20%	14.60%	12%	39%	16%
Programiranje u nekom programskom jeziku	9%	11.40%	7%	16%	7%
Konfigurisanje parametara tokom neke instalacije	27%	6.90%	\	47%	\

Tabela 3 prikazuje podatke o osnovnim radnjama na računaru koje ne podrazumijevaju upotrebu Interneta. Analizom predstavljenih podataka, moglo bi se zaključiti da su znanja i vještine na nivou Crne Gore generalno homogena,

stanovništvo posjeduje osnove znanja na računaru, ali su očigledni nedostaci u: radu sa kalkulacijama, radu sa prezentacijama i promjenama konfiguracionih parametara softverskih aplikacija. Prve dvije aktivnosti se pretežno donose na poslovno okruženje, dok se posljednja odnosi na nivo profesionalnog poznavanja rada na računaru.

U Tabeli 4 su predstavljeni podaci o vrstama aktivnosti na Internetu. i ovdje se može uočiti da postoji prilična usklađenost podataka sa evropskim standardima, s jasno identifikovanim nedostakom znanja o postavljanju i izmjenama parametara bezbjednosti u Internet pretraživaču.

Tabela 4. Pokazatelji znanja/vještina upotrebe Interneta

	EU28 -2012	Crna Gora	Kipar	Luksemburg	Malta
Rad u pretraživaču	75%	72%	64%	91%	66%
Slanje email-a sa prilogom	82%	53%	49%	79%	55%
Postavljanje komentara na forumima	37%	47%	40%	43%	31%
Telefonski pozivi preko Interneta	33%	29%	40%	48%	32%
Prenos fajlova	14%	8%	10%	12%	19%
Kreiranje veb strane	10%	1%	1%	13%	8%
Postavljanje raznih sadžaja na veb	30%	20%	38%	31%	19%
Promjena parametara bezbjednosti u pretraživaču	24%	10%	15%	36%	21%

Pored navedenih indikatora o upotrebi računara i Interneta od strane stanovnika Crne Gore, neophodno je analizirati i aspekat fromalne edukacije i karakteristika obrazovnog sistema. Na osnovu dostupnih podataka može se uočiti da postoji neadekvatna zastupljenost predmeta i programa koji se odnose na znanja i vještine u oblasti sajber bezbjednosti. U planovima i programima za osnovne nivoe obrazovanja, postoji svega nekoliko predmeta koji daju osnovna informatička znanja i vještine (upotrebe računara i Interneta). Za učenike osnovnih i srednjih škola je organizovano nekoliko kampanja od strane Ministartsva prosvjete koje se donose na elemente bezbjednosti upotrebe Interneta. Ipak, kontinuirana edukacija ne postoji na ovom nivou.

S druge strane, univerziteti u Crnoj Gori imaju samo jedan specijalistički i dva master programa u oblasti sajber bezbjednosti (sve na Univerzitetu Donja Gorica), dok na ostalim fakultetima informatičkog i pravnog profila postoji nekoliko predmeta koji analiziraju tehničke i pravne aspekte sajber bezbjednosti. Ipak, nameće se opšti zaključak da ne postoji adekvatna formalna edukacija, pa je evidentan nedostatak edukovanih kadrova specijalizovnih u oblasti sajber bezbjednosti.

Takođe, neke kompanije (obično banke i telekomunikacione kompanije) su organizovale nekoliko obuka za svoje zaposlene o zaštiti podataka, ali ne postoje kontinuirane specijalističke obuke kao ni kampanje za građanstvo o osnovama sajber bezbjednosti.

5. ZAKLJUČAK

U ovom radu su sumirani podaci o znanjima i vještinama rada na računaru i upotrebi Interneta, na osnovu kojih se može kreirati procjena pismenosti u oblasti sajber bezbjednosti na nacionalnom nivou u Crnoj Gori. Podaci pokazuju da mlade generacije sve više koriste Internet, ali da im postojeći obrazovni sistem ne nudi dovoljno znanja o sajber bezbjednosti i zaštiti svojih aktivnosti i podataka na Internetu. S druge strane, iako 94% kompanija koristi Internet u svom poslovanju, njihovi zaposleni ne pokazuju visok nivo poznavanja rada (ukoliko je riječ o starosnoj generaciji iznad 45 god), pa samim time ni osnovne principe sajber zaštite. Prema tome, neophdono je organizovati intenzivne kampanje i treninge, a od obrazvonih institucija se očekuje da izmijene svoje programe i doprinesu osnovnom obrazovanju u ovoj oblasti, a kreiranje spcijalizovanih multidisciplinarnih programa u oblasti sajber bezbjednosti na svim nivoima visokog obrazovanja (od Bachelor do doktorskih) bi obezbijedilo školovanje stručnjaka koji će kasnije biti nosioci sajber bezbjednosti na nacionalnom nivou.

Zahvalnost. U ovom radu su predtsavljeni rezultati Tempus projekta 'Unapređenje obrazovnog sistema u oblasti sajber bezbjednosti u Crnoj Gori- ECESM', br. 544088-TEMPUS-1-2013-1-SI-TEMPUS-JPHES.

LITERATURA

[1] R.Šendelj, F.Lombardi, I.Ognjanović, S.Guarino, "*Cyber Security in Montenegro: Practice, Framework and Challenges*", INFOFEST 2014

[2] K. Zickuhr, „Generations 2010", PewInternet, USA

[3] I.Bandara, F.Ioras, K. MaherI, „*Cyber Security Concerns in E-Learning Education*", Proceedings of ICERI2014 Conference, 17th-19th November 2014, Seville, Spain

[4] *Strategija sajber bezbjednosti Crne Gore* 2013-2017, Podgorica jun 2013.

[5] *Zakon o informacionoj bezbjednosti*, Sl. list CG, br.14 od 17.mart 2010

[6] *Cross-matching of practice in ME with EU standards*, ECESM Report, 2014 (dostupno na: http://ecesm.net/publications-0)

[7] P.A.S. Ralstona, J.H. Grahamb, J.L. Hiebb, „*Cyber security risk assessment for SCADA and DCS networks*", ISA Transactions, Vol 46, Issue 4, 2007, p. 583–594

[8] ISO/IEC 27032:2012, „*Information technology – Security techniques – Guidelines for cyber security", 2012*

[9] Council of Europe, "*Convention on Cybercrime*", Budapest, 23.XI.2001

[10] General Assembly, "*Developments in the field of information and telecommunications in the context of international security"*, UN document A/C.1/66/L.30, 14 October 2011

[11] "*Analysis of the ME cyber security public awareness*", ECESM Report, 2014 [http://ecesm.net/publications-0]

[12] "*Upotreba ICT-a u Crnoj Gori-domaćinstva/lica, preduzeća u 2011*", MONSTAT, 2012