Analiza upoznatosti institucija sa zaštitom IT i IKT sistema na teritoriji opštine Zrenjanin sa fokusom na bežične mreže

Milan Malić, Dalibor Dobrilović
Tehnički fakultet „Mihajlo Pupin“ – Zrenjanin
Univerzitet u Novom Sadu
Zrenjanin, Srbija
milanmalic@outlook.com | dalibor.dobrilovic@uns.ac.rs

Dušan Malić
Visoka tehnička škola
strukovnih studija u Zrenjaninu
Zrenjanin, Srbija
dmalic@sbb.rs

***Sažetak*—Danas, često se mogu pročitati kako medijski tako i naučni članci na temu bezbednosti i zaštite IT i IKT sistema koji ukazuju na probleme sa kojima se susreću poslovne i druge organizacije. Upravo ti problemi mogu biti katastrofalni za njen rad i postojanje. Stoga, neophodno je kreirati model za proveru nivoa upoznatosti odgovornih osoba sa ovom problematikom. Primenom datog modela, a potom i analizom dobijenih rezultata, mogu se izvesti zaključci o stvarnom nivou znanja i upoznatosti poslovnih organizacije sa zaštitom IT i IKT sistema. Istraživanje je bilo motivisano rezultatima prethodnih istraživanja u oblasti sigurnosti bežičnih računarskih mreža. Na kraju rada, prezentuju se buduća istraživanja koja je neophodno sprovesti, kao i akcije koje je neophodno preduzeti radi poboljšanja postojećeg stanja, a na osnovu uočenih nedostataka.**

Keywords—penetraciono testiranje; zaštita podataka; model evaluacije; analiza stanja; zaštita IKT;

I. UVOD

Danas, gotovo da ne postoji poslovna organizacija koje ne primenjuje neki vid IT i IKT tehnologija u svom svakodnevnom poslovanju. Upravo količina podataka koja se skladišti i šalje u digitalnom obliku danas se meri u zettabajtima, pri čemu, po istraživanju [1], očekuje se rast od 2 zettabajtima po godini do 2019. godine. Takođe u radu [2], ističe se da današnje moderne aplikacije su u stvari aplikacije sa visokom funkcionalnošću koje se oslanjaju na razmenu podataka putem IKT i to najčešće u dva pravca, tj. između servera sa jedne strane i klijenta sa druge. Upravo ovakve i slične aplikacije generišu veliku količinu osetljivih i poverljivih podataka koje je neophodno zaštiti od neovlašćenog korišćenja.

Uporedo sa navedenim, ne treba zaboraviti da je upotreba bežičnih tehnologija sve veća, kako u privatnoj, tako i u poslovnoj upotrebi. Na osnovu sprovedenih istraživanja [3, 4], koje su vršena po uzoru na [5, 6], a koja su i ranije postojala u našoj zemlji [7, 8], utvđeno je da je nivo bezbednosti bežičnih mreža nizak. Istraživanja su rađena na širem području Srbije, u kontinuitetu, od 2011. godine, a najviše u Zrenjaninu, Novom Sadu i Beogradu. Takođe, vršena su i uporedna i slična istraživanja, ali u manjem obimu u susednim zemljama [3]. Istraživanja su rađena u skladu sa metodom poznatom kao Wardriving [10, 11], uz upotrebu alata kao što su Wigle [12] i Kismet [13].

Stoga, na osnovu navedenog, u radu će se predstaviti model za evaluaciju upoznatosti odgovornih osoba sa zaštitom IT i IKT sistema, sa izrazitim fokusom na bežične mreže, kao i realizacija analize dobijenih rezultata sprovedene ankete na teritoriji opštine Zrenjanin.

Ekspanzija u razvoju IT i sve češća primena novih dostignuća u ovom polju, čine poslovne organizacije ranjivim bez obzira na njihovu veličinu i budžet kojim raspolažu. Stoga, slobodno se može zaključiti da zaštita novih IT mora biti razmatrana na nekoliko nivoa, počev od individua koje ih razvijaju, pa sve do krajnjih korisnika koji ih implementiraju u svojim postrojenjima. Takođe, treba istaći da zaštita mora biti kontinuirano unapređivana, a novo otkrivene bezbednosne ranjivosti otklanjane u što kraćem vremenskom roku. Upravo ovakva dinamika zahteva kontinuirano unapređenje znanja u domenu zaštite podataka.

Kao primer, navedenom, najbolje svedoči najveći organizovani [*Distributed Denial-of-Service* (DDoS)] napad do sada sproveden uz pomoć kompromitovanih IoT uređaja [3]. Iako ovaj napad nije okrenut ka kompromitovanju osetljivih podataka, njegove posledice mogu biti katastrofalne za poslovanje jedne organizacije ukoliko ona implementira neki vid od navedenih tehnologija kroz svoje svakodnevne aktivnosti. Upravo primena penetracionog testiranja, i uočavanje bezbednosnih ranjivosti u ranim fazama mogu načiniti velike uštede poslovnim organizacijama, pa čak i sprečiti njeno zatvaranje nakon curenja poverljivih podataka.

Autori, su u okviru ovog rada, kreirali model za utvrđivanje nivoa upoznatosti odgovornih osoba sa zaštitom podataka u oblasti bežičnih mreža ali i trenutni nivo bezbednosti bežičnih IT i IKT sistema u poslovnoj organizaciji. Kreirani model je i primenjen kroz anketu na teritoriji opštine Zrenjanin, kako bi se na što efikasniji način analiziralo trenutno stanje. Struktura ankete i detaljnija analiza pitanja biće predstavljena u daljem toku rada.

Prestala poglavlja ovog rada organizovana su po sledećim sekcijama: Sekcija II: Model za utvrđivanje nivoa bezbednosti

IT i IKT sistema, Sekcija III: Struktura organizacija u kojima je sprovedena anketa, Sekcija IV: Anketa o sigurnosti bežičnih mreža u organizacijama, Sekcija V: Rezultati ankete, Sekcija VI: Zaključak i buduća istraživanja.

II. Model za utvrđivanje nivoa bezbednosti IT i IKT sistema

Primenjeni model u ovom radu za cilj postavlja utvrđivanje trenutnog nivoa bezbednosti i znanja odgovornih osoba iz oblasti IT i IKT sistema. S obzirom da je reč o veoma osetljivoj temi i da je malo onih poslovnih organizacija koje bi pristale da otkrije svoje trenutne bezbednosne politike, velika pažnja je posvećena strukturi pitanja. Stoga potrebno je postaviti pitanja na takav način da poslovne organizacije odgovore na što veći broj istih, a da se direktno ili indirektno ne naruši njihova bezbednost. Takođe, potrebno je i zagarantovati anonimnost učesnicima na takav način da njihovi podaci ne bi bili direktno kompromitovani.

Sama struktura modela podeljena je u četiri oblasti, a to su: (A) Identifikovanje poslovne organizacije, (B) Primena penetracionog testiranja, (C) Zaštita IKT sistema, i (D) Želja za promenama. Svaka od navedenih oblasti se sastoji od niza pitanja, čiji je cilj bliže identifikovanje poslovne organizacije i načina njenog poslovanja. U ovom radu prikazan je samo deo ankete sa pitanjima koja su fokusirana na bežične mreže iz razlofa navedenih u uvodnom delu rada.

III. Struktura organizacija u kojima je sprovedena anketa

Kako bi se na najefikasniji način uspostavio profil nivoa zaštićenosti IT i IKT infrastrukture poslovnih organizacija na teritoriji opštine Zrenjanin odabrane se određene oblasti delatnosti koje bi trebalo da skladište najviše poverljivih informacija o svojim klijentima, poslovnim partnerima i samim zaposlenima. Stoga, prilikom kreiranja uzorka sprovedene ankete vodilo se računa da on prestavlja najrealniju sliku strukture poslovnih organizacija na teritoriji opštine Zrenjanin. U tabeli 1. dat je prikaz uzorka izražen u procentima zastupljenih oblasti delatnosti u odnosu na broj zaposlenih u organizacijama nad kojim je sprovedena anketa.

Tabela I. Struktura i veličina organizacija

Veličina org./ Industrija	Proizv.	Obraz.	Javne Ust.	Pruž. Usl.	Trg.	U	(%)
Manje od 5	2	2	0	8	3	15	23.08
6 do 25	0	1	2	7	1	11	16.92
26 do 100	3	2	7	6	1	19	29.23
Vise od 100	4	2	5	5	4	20	30.77
Ukupno	**9**	**7**	**14**	**26**	**9**	**65**	**100**

Kao što se može uočiti iz tabele 1. u anketi je učestvovalo 65 poslovnih organizacija iz 5 različitih oblasti delatnosti počev od proizvodnje (9), obrazovanja (7), javnih ustanova (14), agencija za pružanje usluga (26) (knjigovodstvo, turističke agencije, advokatske kancelarije, itd.) i trgovine (9). Stoga, broj poverljivih podataka slobodno se može zaključiti je na velikom nivou koje ove organizacije čuvaju u digitalnoj formi.

Takođe, iz navedene tabele može se zaključiti da je čak 20 poslovnih organizacija koje su učestvovale u anketi zapošljava više od 100 radnika, što predstavlja više od 30% ispitanika. Upravo ovaj podatak ukazuje na to da veliki broj zaposlenih zahteva i veći nivo celokupne zaštite iz razloga što u ovakvim slučajevima potencijalni nivo rizika raste sa mogućnošću da zlonamerni napadi poteknu upravo iz same organizacije. Isto tako može se uočiti da kada je reč o broju zaposlenih procenat je ravnomerno raspoređen između učesnika, gde preko 23% anketiranih spada u male organizacije, dok oko 46% ispitanika spada u srednje sa brojem zaposlenih od 6 do 100.

IV. Anketa o sigurnosti bežičnih mreža u organizacijama

Razvoj IKT sistema proteklih godina je bio fokusiran na usavršavanje i obezbeđivanje komunikacionih protokola i standarda, a sve sa ciljem povećanja bezbednosti i protoka podataka. Stoga naučnici širom sveta koriste razne vidove metodologija i tehnika kako bi utvrdili stvarno stanje i preduzeli odgovarajuće korake s ciljem poboljšavanja i usavršavanja.

Primena bežičnih mreža u poslovnim organizacijama, danas, je sve veća i veliki broj poslovnih organizacija ih koristi. Na ovaj način organizacije obezbeđuju veliki broj prednosti svojim zaposlenim ali i stavljaju svoje IKT sisteme u nebezbedno stanje.

Upravo se kroz ovu grupu pitanja želi ustanoviti u kojoj meri poslovne organizacije na teritoriji opštine Zrenjanin primenjuju bežične mreže. Takođe, želi se ustanoviti koji nivoi zaštite se primenjuju na tim bežičnim mrežama i šta sve odgovorne individue čine da bi učine bežične sisteme bezbednijim. Ovom prilikom postavljena su sledeća pitanja:

(1) Da li organizacija koristi bežične mreže u svom poslovanju?

(2) Ukoliko se primenjuju, koji vid enkripcije se koristi od navedenih?

(3) Da li bežična mreža emituje otvoreno SSID?

(4) Prilikom kreiranja šifre, za pristup bežičnoj mreži, koji karakteri se koriste?

(5) Sigurnosna šifre (bezbednosne fraze), koja se implementira kroz bežične mreže, koliko ima karaktera?

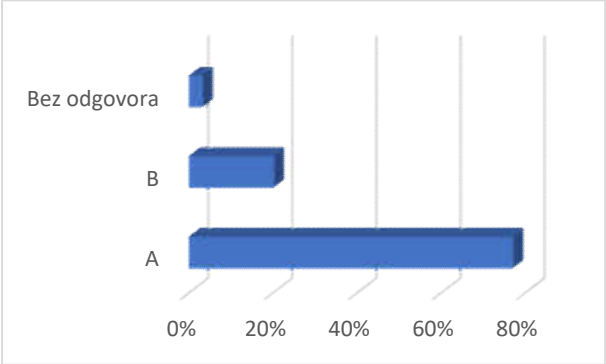
(6) Prilikom kreiranja šifre da li se koriste upravitelji šiframa ili specijalni algoritmi za njihovo generisanje i bezbedno skladištenje?

V. Rezultati ankete

Kao što je ukazano u prethodnom sekciji prvim pitanjem u sprovedenoj anketi želi se ustanoviti da li postoji i u kojoj meri primena bežičnih tehnologija u poslovanju organizacije. Na slici 1. dat je grafički prikaz rezultata, a u tabeli II. statistička analiza istih na osnovu veličine organizacije, na postavljeno pitanje.

TABELA II. PRIKAZ ODGOVORA NA PITANJE BR.1

Veličina organizacije	DA	NE	Bez odgovora	Ukupno
Manje od 5	13	2	0	
6 do 25	10	1	0	
26 do 100	14	4	1	
Vise od 100	13	6	1	
Ukupno	**50**	**13**	**2**	**65**



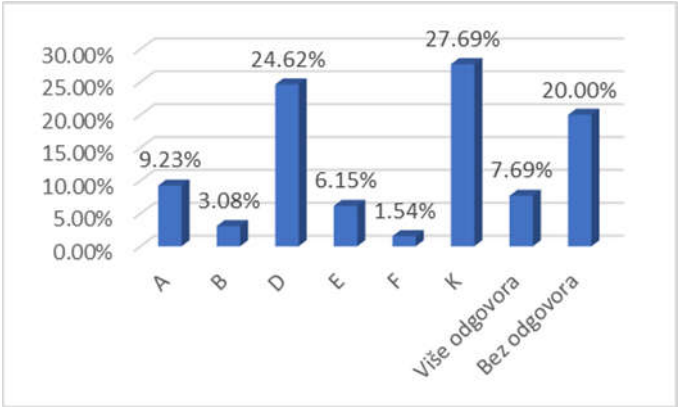
Slika 1. Rezultati ankete po procentima za pitanje br. 1

Kao što se može uočiti sa slike 1. 76.92% anketiranih poslovnih organizacija je odgovorilo na ponuđeni odgovor pod A, a što ukazuje na primenu bežičnih mreža u sastavu svojih IKT sistema. S druge strane 20% ispitanika je zaokružilo odgovor pod B i time ukazalo da ne primenjuje nikakav vid bežičnih tehnologija prilikom svog poslovanja. Na postavljeno pitanje 3.08% ispitanika je odbilo da odgovori. Stoga se na osnovu navedenog nedvosmisleno može zaključiti da veliki broj poslovnih organizacija u opštini Zrenjanin primenjuje bežične mreže.

Kao što se može uočiti iz tabele II. primena bežičnih mreža u poslovnim organizacijama opada sa veličinom same organizacije. Razlog se ogleda u tome što fizička površina organizacije se povećava srazmerno broju zaposlenih pa samim tim i troškovi u implementaciji infrastrukture ali i održavanju iste rastu.

S druge strane kako bi se utvrdila bezbednosti bežičnih mreža neophodno je sagledati dva aspekta, a to su koji vid enkripcije se primenjuju i jačina sigurnosne fraze (šifre). Pitanje br. 2. u sprovedenoj anketi se odnosi na to koji vid enkripcije koji poslovne organizacije primenjuju na implementiranim bežičnim mrežama. Slika 2. prikazuje analizu odgovora na ovo pitanje, dok tabele III, IV i V sagledavaju statističku analizu odgovora po veličini organizacije. Reference koje bolje objašnjavaju sigurnosne mehanizme u bežičnim mrežama, tj. WPA, WPA2, AES i dr., su [14, 15, 16, 17, 18].

Kada je reč o tome koji vid enkripcije se primenjuje nad bežičnim mrežama (Slika 2.) ispitanici su najviše, u udelu od 24.62%, odgovorili da primenjuju WPA2 što se smatra bezbednim enkripcijom. Takođe, kada je reč o bezbednim sigurnosnim nivoima treba reći da je 6.15% ispitanika odgovorilo da primenjuje WPA2 Enterprise, a 1.54% da primenjuje AES.



Slika 2. Rezultati ankete po procentima za pitanje br. 2

TABELA III. PRIKAZ ODGOVORA NA PITANJE BR.2

Veličina organizacije	Ne primenjuje se	WEP	WPA	WPA2	WPA2 Ent
Manje od 5	2	0	0	4	0
6 do 25	1	1	0	1	1
26 do 100	1	0	0	7	1
Vise od 100	2	1	0	4	2
Ukupno	**6**	**2**	**0**	**16**	**4**

TABELA IV. PRIKAZ ODGOVORA NA PITANJE BR.2

Veličina organizacije	AES	LEAP	CCMP	802.11i	EAP
Manje od 5	0	0	0	0	0
6 do 25	1	0	0	0	0
26 do 100	0	0	0	0	0
Vise od 100	0	0	0	0	0
Ukupno	**1**	**0**	**0**	**0**	**0**

TABELA V. PRIKAZ ODGOVORA NA PITANJE BR.2

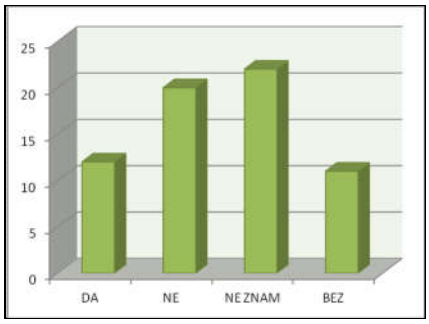
Veličina organizacije	NE znam	Drugo	Višestruki	Bez enkripcije
Manje od 5	7	0	0	2
6 do 25	4	0	1	1
26 do 100	4	0	2	4
Vise od 100	3	0	2	6
Ukupno	**18**	**0**	**5**	**13**

Ipak, zabrinjavajuće se da je čak 27.69% odgovornih lica odgovorilo da ne zna koji vid enkripcije se koristi i da li se uopšte neki koristi. Ovo je samo još jedan pokazatelj koji ukazuje na loše poznavanje zaštite i osiguravanja IT i IKT sistema kod ispitanika. Takođe, alarmantna je činjenica da je 9.23% ispitanika ukazalo da ne primenjuju svesno nikakav vid zaštite, a da je 3.08% ukazalo da primenjuje WEP enkripciju. Stoga se na osnovu navedenog može zaključiti da je gotovo 40% bežičnih mreža potencijalno neobezbeđeno kada su u pitanju poslovne organizacije na teritoriji opštine Zrenjanin.

Po mnogim autorima u polju bezbednosti IKT sistema otvoreno emitovanje SSID se smatra bezbednosnom ranjivošću. S druge strane, danas, postoji veliki broj alata koji lako detektuju sakrivene bežične mreže i ovaj sigurnosni mehanizam lako zaobilaze. Na slici 3. dat je grafički prikaz analize odgovora na postavljeno pitanje, a u tabeli VI. statistička analiza na osnovu veličine organizacije.

TABELA VI. PRIKAZ ODGOVORA NA PITANJE BR.3

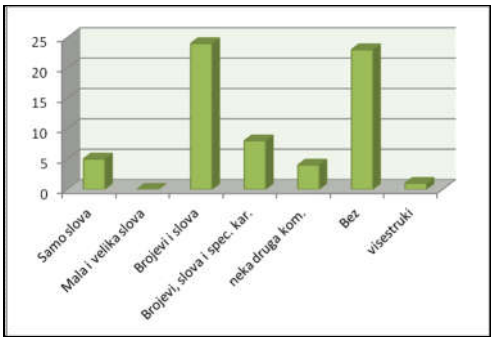
Veličina organizacije	DA	NE	NE ZNAM	BEZ	
Manje od 5	2	2	10	1	
6 do 25	4	3	3	1	
26 do 100	4	6	5	4	
Vise od 100	2	9	4	5	
Ukupno	**12**	**20**	**22**	**11**	**65**



Slika 3. Rezultati ankete po procentima za pitanje br. 3

Na pitanje „Da li bežična mreža emituje otvoreno SSID?“ (Slika 3.)) 18.46% ispitanika je odgovorio sa da. S druge strane 30.77% ispitanika je odgovorio da njihova mreža ne emituje otvoreno SSID. Ipak, veliki broj njih čak 33.85% je odgovorio da ne zna o čemu je reč. Kroz tabelu VI. data je statistička analiza odgovora na ovo pitanje, a pri čemu je za osnov uzeta veličina organizacije.

Druga bitna komponenta kada je upitanju sigurnost bežičnih mreža, kao što je rečeno, jeste sigurnosna fraza, odnosno, šifra za pristup. Za utvrđivanje bezbednosnog nivoa šifre se uglavnom koriste dve komponente, a to su koja kombinacija karaktera se koristi i dužina šifre. Na slici 4. dat je grafički prikaz odgovora na postavljeno pitanje o primenjenoj kombinaciji karaktera, a kroz tabele VII i VIII statistička analiza rezultata na osnovu veličine organizacije.



Slika 4. Rezultati ankete po procentima za pitanje br. 4

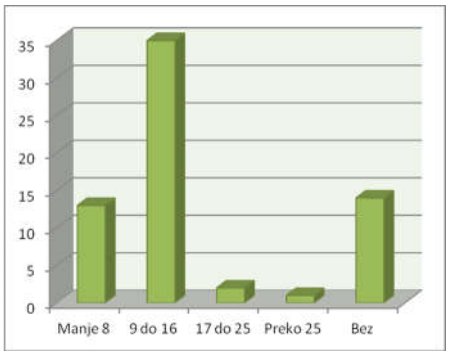
TABELA VII. PRIKAZ ODGOVORA NA PITANJE BR.4

Veličina organizacije	Samo slova	Mala i velika slova	Brojevi i slova	Brojevi, slova i spec. karakteri
Manje od 5	0	0	9	3
6 do 25	1	0	5	3
26 do 100	2	0	7	0
Vise od 100	2	0	3	2
Ukupno	5	0	24	8

TABELA VIII. PRIKAZ ODGOVORA NA PITANJE BR.4

Veličina organizacije	Neka druga kombinacija	Bez	Viseštruki	Ukupno
Manje od 5	1	2	0	
6 do 25	0	2	0	
26 do 100	2	7	1	
Vise od 100	1	12	0	
Ukupno	4	23	1	65

Kada je reč o kombinaciji karaktera rezultati odgovora na ovo pitanje su prikazani na slici 4. Najveći broj ispitanika je odgovorio, njih 36.92%, da koristi brojeve i slova prilikom kreiranja šifri za bežične mreže, a 12.31% kombinaciju slova, brojeva i specijalnih karaktera. Slabe šifre koje se sastoje samo od slova sačinjene su u 7.69% slučajeva. Ovom prilikom treba istaći da 35.38% ispitanika nije odgovorilo na ovo pitanje, iz razloga što ne primenjuju bežične mreže ili pak njihove mreže ne koriste bezbednosni mehanizam koji zahteva upotrebu šifre.



Slika 5. Rezultati ankete po procentima za pitanje br. 5

S druge strane, kada je reč o dužini šifre (Slika 5.) najveći broj ispitanika, njih 53,85% se izjasnio da koristi šifre u dužini od 9 do 16 karaktera, što predstavlja srednji nivo šifre. S druge strane svega 6.15% ispitanika je zaokružio odgovor koji ukazuje na slabe šifre, a to je da one imaju manje od 8 karaktera. Ipak, bilo je poslovnih organizacija koje implementiraju i jake šifre koje se sastoje od 17 od 25 karaktera. Ovom prilikom treba naglasiti da nije bilo ispitanika koji koriste ekstremno jake šifre koje se sastoje od 25 i više karaktera. Preostali ispitanici nisu odgovorili na ovo pitanje.

TABELA IX. PRIKAZ ODGOVORA NA PITANJE BR.5

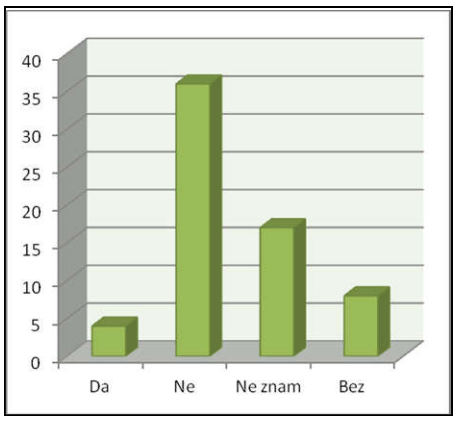
Veličina organizacije	manje 8	9 do 16	17 do 25	preko 25	bez	
Manje od 5	5	8	0	0	2	
6 do 25	2	8	0	0	1	
26 do 100	3	11	1	0	4	
Vise od 100	3	8	1	1	7	
Ukupno	**13**	**35**	**2**	**1**	**14**	**65**

Na kraju, kako bi se utvrdila indirektna struktura bezbednosnih fraza, postavljeno je pitanje: „Da li se prilikom kreiranja šifre koriste se upravitelji šiframa ili specijalni algoritmi za njihovo generisanje i bezbedno skladištenje?“. Na ovaj način se želelo utvrditi da li se koriste šifre iz svakodnevnog života, koje su podložne socijalnom inženjeringu ili napadima uz pomoć rečnika, ili se, pak, koriste specijalizovani alati za skladištenje i generisanje šifri. Ovom prilikom je 26.15% korisnika odgovorilo da nije upoznato sa

ovim vidom aplikacija, a 55.38% je odgovorilo da ih ne koristi. Svega 6.15% ispitanika je odgovorilo da primenjuje ovaj vid aplikacija za generisanje i skladištenje šifri. Treba napomenuti da 12.31% ispitanika nije odgovorio na ovo pitanje.

TABELA X. PRIKAZ ODGOVORA NA PITANJE BR.6

Veličina organizacije	**Da**	**Ne**	**Ne znam**	**Bez**	
Manje od 5	0	8	6	1	
6 do 25	1	8	2	0	
26 do 100	1	10	5	3	
Vise od 100	2	10	4	4	
Ukupno	**4**	**36**	**17**	**8**	**65**



Slika 6. Rezultati ankete po procentima za pitanje br. 6

Može se zaključiti, na osnovu pitanja i odgovora iz ovog dela Ankete, da veliki broj poslovnih organizacija, njih ¾, primenjuje bežične mreže prilikom svog poslovanja. Ipak, jako je mali broj onih koji podižu nivo bezbednosti na najviši mogući za iste i time vrše zaštitu svojih IKT sistema. Takođe, treba naglasiti da je veliki broj onih koji primenjuju slabe ili relativno slabe šifre za pristup svojim mrežama. Ovo dovodi do sveobuhvatne loše bezbednosne strukture IT sistema, čime isti postaju podložni zlonamernim napadima i kompromitovanju od strane zlonamernih napadača. Stoga, potrebno je načiniti velike napore po pitanju edukovanja zaposlenih i odgovornih lica iz ove oblasti.

VI. ZAKLJUČAK

Kao što se može zaključiti na osnovu navedenog istraživanja, predstavljenog kroz rad, mogućnost kreiranja modela za proveru nivoa upoznatosti odgovornih osoba sa zaštitom IT i IKT sistema je moguć. Upravo predloženi model, u ovom radu, primenjuje ne agresivnu metodu za utvrđivanje upoznatosti odgovornih osoba sa datim domenom.

Iako je navedena problematika česta među poslovnim organizacijama koje primenjuju IT i IKT sisteme u svom svakodnevnom poslovanju, na osnovu sprovedenog istraživanja može se zaključiti da zaštita upravo ovih sistema nije na visokom nivou. Veliki broj organizacija primenjuje u nekom segmentu bežične mreže u svojoj infrastrukturi i pritom ostavlja iste ranjivim za napade. Stoga, upravo ovakve slabo zaštićene mreže postaju prva faza u napadu na te poslovne organizacije. Poslovne organizacije često pribegavaju jednostavnijim rešenjima i slabijim infrastrukturnim rešenjima, a sve sa ciljem smanje budžeta postavljajući time bezbednost i zaštitu u drugi plan. Na navedeno najbolje ukazuju politike za kreiranje šifri gde ispitanici odgovaraju na to da koriste kompleksne šifre, koje sadrže do 16 karaktera, ili isto tako ne primenjuju aplikacije za njihovo bezbedno čuvanje. Upravo navedeno nedvosmisleno ukazuje da kompleksnost šifri se stavlja u drugi plan i da se koriste fraze iz svakodnevnog života koje su lake za pamćenje.

Stoga, na osnovu navedenih rezultata, može se zaključiti da poslovne organizacije u budućnosti moraju posvetiti više pažnje i sredstava u domenu zaštite njihove digitalne infrastrukture. Takođe, veoma je bitno naglasiti da je prilikom sprovođenja navedenog istraživanja veliki broj ispitanika pristupio istom sa velikim entuzijazmom i željom da učestvuje u istraživanju, a sve sa ciljem da se detaljnije upozna sa ovom problematikom. Upravo navedeno ukazuje na činjenicu da su poslovne organizacije svesne da je neophodno da izvrše promene u svom poslovanju i posvete više pažnje zaštiti, kako sopstvene infrastrukture tako i podataka koje čuvaju o svojim klijentima.

LITERATURA

[1] Cisco Visual Networking Index: Forecast and Methodology, (2014-2019) Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html.

[2] The Rise of the Networked Enterprise: Web 2.0 finds its payday, Available: http://www.mckinsey.com/industries/high-tech/our-insights/the-rise-of-the-networked-enterprise-web-20-finds-its-payday. K. Elissa, “Title of paper if known,” unpublished.

[3] Dalibor Dobrilovic, Zeljko Stojanov, Stefan Jäger, Zoltán Rajnai, A Method for Comparing and Analyzing Wireless Security Situations in Two Capital Cities, Acta Polytechnica Hungarica, Vol. 13, No. 6, pp. 67-86, 2016, ISSN 1785-8860, , DOI: 10.12700/APH.13.6.2016.6.4.

[4] Dalibor Dobrilovic, Borislav Odadzic, Zeljko Stojanov, Zlatko Covic, Approach in IEEE 802.11 security analytics and its integration in university curricula, 3rd International Conference & Workshop Mechatronics in Practice and Education - MECHEDU 2015, pp. 41-46, 14 – 16 May, Subotica, Serbia, 2015.

[5] Ionescu, V.; Smaranda, F.; Sima, I.; Diaconu, A., ―Current status of the wireless local area networks in Romania,‖ Roedunet International Conference (RoEduNet), 2013 11th , vol., no., pp.1,4, 17-19 Jan. 2013.

[6] Nisbet, A., ―A tale of four cities: Wireless security & growth in New Zealand,‖ Computing, Networking and Communications (ICNC), 2012 International Conference on , vol., no., pp.1167,1171, Jan. 30 2012-Feb. 2 2012.

[7] Dušan Švenda, Miroslav Djordjević, Mapping of IEEE 802.11 wireless networks in Belgrade (In Serbian: Mapiranje IEEE 802.11 bežičnih mreža u Beogradu), 18. Telecommunication forum TELFOR 2010 Serbia, Belgrade, November 23.-25., 2010.

[8] Saša Adamović, Marko Šarac, Dalibor Radovanović, Wireless Network IEEE 802.11 Security Analysis on the area of city of Belgrade (In Serbian: Analiza sigurnosti bežičnih mreža IEEE 802.11 na teritoriji grada Beograda, INFOTEH-JAHORINA Vol. 10, Ref. B-III-1, p. 191-194, Bosnia and Herzegovina, Martch 2011.

[9] http://www.networkworld.com/article/3123672/security/largest-ddos-attack-ever-delivered-by-botnet-of-hijacked-iot-devices.html

[10] C. Hurley, R. Rogers, F. Thompson, D. Connelly, B. Baker: WarDrivingand Wireless Penetration Testing, Syngress Publishing, Inc. Rockland, USA, 2007

[11] Hira Sathu: Wardriving: technical and legal context. In Proceedings of the 5th WSEAS international conference on Telecommunications

andinformatics (TELE-INFO'06), Stevens Point, Wisconsin, USA, pp. 162-167, 2006

[12] Wigle - http://www.wigle.net, seen on 2016.03.12

[13] Haines, B., Thornton, F.: Kismet Hacking, Syngress Publishing, 2008

[14] Chris Hurley, Frank Thorton, Michael Puchol, Russ Rogers: WarDriving: Drive, Detect, Defend: A Guide to Wireless Security, Syngress Publishing, Inc., Rockland, USA, 2004

[15] David D. Coleman, David A. Westcott, Bryan E. Harkins, Shawn M. Jackman: CWSP® Certified Wireless Security Professional Official – Study Guide, Wiley Publishing, Inc., Indianapolis, USA, 2010

[16] Gary A. Donahue: Network Warrior, O'Reilly Media, Inc., Sebastopol, USA, 2011

[17] Mark Ciampa: CWNA Guide to Wireless LANs, Course Technology, Cengage Learning, USA 2013

[18] Eric Cole, Ronald Krutz, James W. Conley: Network Security Bible, Wiley Publishing, Inc., Indiana, USA, 2005.

ABSTRACT

Abstract—Today, frequently the articles in news and scientific publications appear regarding the topics of IT and ICT systems security which point out the problems facing business and other institutions. These problems can be catastrophically for their business and existence. Therefore, it is necessary to create model for checking the awareness of personnel responsible for these issues. With the application of the given model, and with the analyses of obtained results, the conclusions can be drawn about real level of knowledge and institutional awareness regarding IT and ICT systems security. This research has been motivated with previous researches in the area of wireless network security. At the end of this paper, the future directions of research necessary to apply are presented, as well as the actions in order to improve the current security situation, on the basis of identified weaknesses.

Keywords—penetration testing; data security; evaluation model; situation analyses; ICT security;

ANALYSES OF INSTITUTIONAL AWARNESS OF IT AND ICT SYSTEMS SECURITY ISSUES IN THE AREA OF CITY OF ZRENJANIN WITH THE FOCUS ON WIRELESS NETWORKS

Milan Malić, Dalibor Dobrilović, Dušan Malić