VARSTVOSLOVJE,
let. 15
št. 3
str. 338–356

Percepcija kibernetske kriminalitete pri nekaterih uporabnikih interneta v Sloveniji in ZDA

Maja Dimc, Bojan Dobovšek

Namen prispevka:

Namen prispevka je analizirati problematiko kibernetske kriminalitete kot sodobne varnostne grožnje v povezavi z ozaveščenostjo in delovanjem posameznika v kibernetskem prostoru. Na podlagi empirične raziskave, izvedene v Sloveniji in Združenih državah Amerike, je izpostavljena problematika ozaveščenosti splošne javnosti na področju kibernetske kriminalitete v povezavi z njihovim preventivnim delovanjem v kibernetskem prostoru in odnosom do organov pregona s ciljem opredelitve ključnih razlik med percepcijo, vedenjem in delovanjem posameznikov glede na njihovo fizično življenjsko okolje (Slovenija in ZDA).

Metode:

Za potrebe prispevka je bila izvedena empirična raziskava, ki je vključevala dve skupini anketirancev, in sicer skupino posameznikov v Sloveniji ter skupino posameznikov v ZDA. Uporabljeno je bilo neeksperimentalno raziskovanje; za zbiranje podatkov je bil uporabljen anketni vprašalnik, s katerim smo merili poznavanje problematike, stališča in vedenje posameznikov v povezavi s pojavom kibernetske kriminalitete.

Ugotovitve:

Raziskava je pokazala pomembno razliko med ozaveščenostjo posameznikov in njihovim dejanskim varnostnim ravnanjem v virtualnem okolju, ki se v osnovi ne razlikuje glede na fizično lokacijo posameznika. Drugače pa je z občutkom varnosti, kjer se fizična lokacija preslika v virtualno okolje, saj so anketiranci živeči in delujoči v manjši državi (Slovenija) izrazili višjo stopnjo občutka varnosti v virtualnem okolju kot anketiranci živeči in delujoči v večji državi (Združene države Amerike). Poleg tega je bilo v okviru raziskave ugotovljeno, da obstaja nezaupanje in skepticizem glede usposobljenosti organov pregona za obravnavo primerov kibernetske kriminalitete, kar se odraža v potencialno manjši verjetnosti prijave in posledične obravnave kaznivih dejanj kibernetske kriminalitete. Z vidika ozaveščanja splošne javnosti s ciljem dosega visokega nivoja varnostnega ravnanja bi bilo potrebno povečati količino aktivnosti, povezanih z ozaveščanjem, hkrati pa bi se morali posvetiti tudi aktivnostim, ki bi zviševale stopnjo zaupanja v delovanje organov pregona.

Omejitve/uporabnost raziskave:

Omejitev raziskave izhaja iz načina zbiranja podatkov, saj je bila uporabljena metoda snežne kepe. Število udeležencev pri raziskavi je bilo dokaj majhno, zato bi bilo nadaljnje raziskave priporočljivo razširiti v smislu vključenosti večjega dela populacije.

Praktična uporabnost:

Rezultati raziskave imajo praktično vrednost na področju implementacije procesov preprečevanja kibernetske kriminalitete, in sicer primarno ozaveščanja splošne javnosti glede pomena lastne informacijske varnosti, saj je bil v okviru raziskave potrjen pomemben razkorak med znanjem in dejansko implementacijo osnovnih tehnik zagotavljanja informacijske varnosti.

Izvirnost/pomembnost prispevka:

Prispevek obravnava problematiko kibernetske kriminalitete in informacijske varnosti v Sloveniji in ZDA, pri čemer poskuša ugotoviti ključne razlike med varnostnim vedenjem in delovanjem posameznikov glede na fizično življenjsko okolje. Ugotovitve raziskave predstavljajo izhodiščno točko za nadaljnje raziskave pojavnosti kibernetske kriminalitete in implementacije informacijske varnosti.

UDK: 343.9:004

Ključne besede: kibernetska kriminaliteta, informacijska varnost, informacijsko-komunikacijske tehnologije, informacijska varnostna kultura

Perception of Cybercrime by Selected Internet Users in Slovenia and USA

Purpose:

The purpose of the article is to analyze the issue of cybercrime as a contemporary security threat as it relates to awareness levels and behavior of an individual in the cyberspace. Based on the empirical research performed in Slovenia and United States of America, the article discusses the issue of user awareness in the field of cybercrime, their consequent preventive behavior in the cyberspace, and their attitude toward law enforcement agencies with the aim of establishing the crucial differences between perception, knowledge and actual behavior of individuals based on their physical everyday environment (Slovenia and USA).

Design/Methods/Approach:

For the purpose of this article, an empirical research involving two groups of participants, a group of individuals from Slovenia and a group of individuals from the United States of America, was performed. Non-experimental research method was used; a survey questionnaire was used for collection of data regarding the level of familiarity, opinion and behavior of individuals as it relates to the issue of cybercrime.

Findings:

The research found an important discrepancy between the level of awareness regarding online safety and the actual behavior of individuals in the virtual environment, which does not differ due to the physical location of the individual. However, when it comes to the feeling of safety, the physical location of an

individual influences his/her feeling of safety while in cyberspace; namely, the research found that the participants living and working in a small country (Slovenia) are also feeling safer in the virtual environment than do the participants living and working in a large country (United States of America). Furthermore, in the framework of this research, we found a concerning level of distrust and skepticism regarding the investigative capabilities of law enforcement in the field of cybercrime, which results in potentially lower reporting rate and consequent lower level of prosecution cases. In terms raising the level of awareness of the general public with the aim of reaching a high level of safeguarding behavior, the level of activities related to awareness, as well as activities related to raising the level of trust in the capabilities of law enforcement, should be increased.

Research Limitations/Implications:

Research limitations are primarily due to the manner of data collection, since we used the snowball sampling method. Additionally, the number of participants if rather low; therefore, further research should be broadened in order to include a wider population range.

Practical Implications:

The research results have practical value in the field of the implementation of the processes of cybercrime prevention, and primarily in the field of raising the level of awareness of the general public regarding the importance of personal information safety, since our research confirmed a discrepancy between the level of knowledge and the level of actual implementation of the basic techniques of information safety assurance.

Originality/Value:

The article discusses the issue of cybercrime and information security in Slovenia and the United States of America. We attempted to find the key differences between safeguarding knowledge and behavior of individuals based on their physical living environment. The findings of the research represent a starting point for further comparison of the incidence of cybercrime and implementation of information security.

UDC: 343.9:004

Keywords: cybercrime, information assurance, information communication technologies, information security culture

1 UVOD

Informacijsko-komunikacijske tehnologije (IKT) ključno vplivajo na delovanje sodobne družbe kot celote. Z razvojem interneta in svetovnega spleta se je razvil kibernetski oz. virtualni prostor, ki se vedno bolj prepleta s fizičnim prostorom. Skupaj s širjenjem funkcionalnosti svetovnega spleta se eksponentno povečuje količina uporabnikov[1] ter tudi vključevanje najrazličnejših naprav v kibernetski

1 *Število uporabnikov interneta se je, zaradi preproste uporabe in eksponentne rasti ponujenih informacij, od leta 2000 do leta 2012 v svetovnem merilu povečalo za 566 % in je v letu 2012 preseglo*

prostor in se dejansko premikamo v smeri omreženja celotne družbene infrastrukture[2]. Prednosti pa s seboj prinašajo tudi določene slabosti in ranljivosti, saj kot pravi Kanduč (v Kovačič et al., 2010: 1) »tehnologija povečuje družbeno in človeško moč in silo, obenem pa tudi odvisnost, nebogljenost in vsakovrstne utvare«.

Informacijsko-komunikacijska tehnologija je, v kombinaciji z delovanjem v kibernetskem prostoru, postala del vsakdanjega življenja, hkrati pa se delovanje organizacij in posameznikov v kibernetskem prostoru ni primerno prilagodilo. Prednosti IKT, kot so dostopnost, povezljivost, razširjenost, avtomatizacija ter seveda prostorska in časovna neomejenost, so lahko tudi največje pasti (Britz, 2009; Dimc, 2009; Taylor, Caeti, Loper, Fritsch in Liederbach, 2006; Wall, 2007). Ključne značilnosti kibernetskega prostora, kot so odsotnost mej, hitrost razvoja, anonimnost akterjev ter avtomatske metode, se hkrati uvrščajo med temeljne značilnosti kibernetskih groženj (Dunn, 2005). Ob tem pa virtualni vidik kibernetskega prostora deluje potencialno zavajajoče, saj se delovanje v takšnem okolju prepogosto dojema kot zgolj virtualno in posledično brez bistvenega vpliva na resnični svet. Shea (2004) tako poudarja, da elektronska naprava deluje kot vmesnik, zaradi katerega se zmanjša percepcija posledic dejanj, izvedenih v kibernetskem prostoru. Na neki način se torej zabriše meja med resničnim in fantazijskim ter ustvari »disinhibicijski učinek«, posledično uporabniki ne čutijo odgovornosti za svoja dejanja v kibernetskem prostoru, četudi gre za nasilno in v resničnem svetu nesprejemljivo vedenje (Suler, 2004). Kljub temu pa sta tako informacijsko-varnostna ozaveščenost in usposobljenost kot tudi človeški vidik informacijske varnosti še vedno le redko obravnavana (Dlamini, Eloff in Eloff, 2009).

Količina kibernetske kriminalitete narašča skupaj s količino ponujenih funkcionalnosti v kibernetskem prostoru in širjenjem uporabe interneta. Uporaba interneta v Sloveniji in ZDA je primerljiva, in sicer je v Sloveniji v letu 2012 internet uporabljalo 70 % prebivalcev (Raba interneta v Sloveniji, 2011), v ZDA pa 78 % prebivalcev (Miniwatts Marketing Group, 2013). V Sloveniji je število prijavljenih incidentov od leta 2008 do leta 2012 naraslo za skoraj 300 % (SI-CERT, 2012), medtem ko se število prijavljenih incidentov v ZDA v teh letih sicer ni bistveno spremenilo, le za dobrih 5 %, vendar pa se je povečala nastala finančna škoda (Internet Crime Complaint Center, 2008, 2012). Glede na populacijo v izbranih državah je število prijav primerljivo, in sicer v Sloveniji 0,14 %, v ZDA pa 0,09 %. Število prijavljenih napadov ribarjenja za podatki in goljufij je Sloveniji v enem letu naraslo kar za 100 % (SI-CERT, 2012), tudi v ZDA so takšne oblike kibernetske kriminalitete v porastu, in sicer je bilo v letu 2012 prijavljenih kar 14.141 primerov goljufij z uporabo elektronske pošte, pri čemer je prišlo do finančne škode več kot 4 milijone USD (Internet Crime Complaint Center, 2012).

V okviru predstavljene raziskave smo poskušali analizirati delovanje posameznika v kibernetskem prostoru glede na njegovo poznavanje in razumevanje

2,4 milijarde (Miniwatts Marketing Group, 2013).

2 *Gre za povezavo širokega spektra fizičnih naprav z internetom (npr. semaforji, elektronski prometni znaki, gospodinjski aparati itd.), kar poimenujemo »internet stvari«, ki omogoča dostop do oddaljenih podatkov in izvajanje fizičnega nadzora ne glede na lokacijo (Kopetz, 2011).*

pojava kibernetske kriminalitete, s tem povezano preventivno delovanje in odnos do organov pregona ter ugotoviti ključne razlike med vedenjem in delovanjem posameznikov v manjši državi (Sloveniji), kjer smo predpostavljali, da se uporabniki počutijo varnejše, in večji državi (ZDA), kjer smo predpostavljali večjo občutljivost posameznikov glede potencialnih nevarnosti. Ugotovitve raziskave predstavljajo izhodiščno točko za nadaljnje primerjave pojavnosti kibernetske kriminalitete in implementacije informacijske varnosti v prihodnosti.

Varnost v povezavi z informacijsko-komunikacijskimi tehnologijami običajno povezujemo s tveganji, pri čemer varnostno tveganje dejansko pomeni razmerje med tveganjem in nevarnostjo; posameznik je tisti, ki odloča o tveganju na podlagi lastne presoje, kar posledično vpliva na njegova dejanja (Rančigaj, 2010). V kibernetskem prostoru se posamezniki sicer zavedajo potencialnih tveganj, vendar jih v veliki meri ne percipirajo kot realne nevarnosti[3]. Posledično so varnostni incidenti v povezavi z informacijsko-komunikacijskimi tehnologijami v veliki meri rezultat neprimernega vedenja, neznanja, neozaveščenosti, ki pretvori obstoječo grožnjo v realno nevarnost.

Razvoj informacijsko-komunikacijskih tehnologij in oblikovanje sodobnega kibernetskega prostora nedvomno vpliva na družbene konstrukte in zaznavo stvarnosti, saj le-ta v kibernetskem prostoru ni niti lokacijsko niti časovno omejena. Ob tem se je treba zavedati, da ima danes posameznik, preko uporabe sodobnih tehnologij, možnost fizičnega, elektronskega ter tudi psihološkega vplivanja na stabilnost ključne informacijske infrastrukture in družbe kot celote (Hundley et al., 2007). Hkrati pa je zaščita sodobnih informacijsko-komunikacijskih tehnologij večplasten postopek (Markelj in Bernik, 2011), ki mora vključevati tako tehnične kot tudi sociološke vidike zagotavljanja varnosti.

Sodobna varnostna paradigma se osredotoča na tri ključne dileme, in sicer referenčne objekte varnosti (na koga se varnost nanaša), grožnje varnosti (kdo ali kaj to varnost ogroža) in varnostne mehanizme (kako varnost zagotavljati) (Liotta v Svete, 2005). V povezavi s sodobnimi tehnologijami ugotavljamo, da posameznik igra pomembno vlogo v vsakem od teh referenčnih objektov, saj se zagotavljanje varnosti nedvomno nanaša na posameznika, hkrati pa je ravno posameznik tisti, ki lahko namerno ali pa nenamerno predstavlja ključno varnostno grožnjo, zato je za zagotavljanje varnosti ključnega pomena okrepiti najšibkejši člen verige – posameznika. Ravno posameznik namreč predstavlja najpomembnejši del varnostnega procesa in »ključ do učinkovite stopnje informacijske varnosti« (Lobnikar, Prislan, Markelj in Banutai, 2012).

Pojem kibernetske kriminalitete je v uporabi že nekaj časa, vendar pa še vedno ni opredeljen dejanski obseg pojava, niti ni vzpostavljena enotna definicija, kar nedvomno negativno vpliva tako na preprečevanje kot tudi pregon (Gordon in Ford, 2006). Problematiko postavitve jasne definicije lahko pripišemo hitremu razvoju oblik kibernetske kriminalitete, ki se je v kratkem obdobju 20-ih let razvila od preprostih oblik zlorabe informacijsko-komunikacijskih tehnologij za

3 *Razliko med percepcijo tveganja in realno nevarnostjo Flaker (1994) zanimivo ponazori s primerom bananinega olupka, in sicer bananin olupek na tleh predstavlja grožnjo, da nam spodrsne in pademo, vendar pa olupek na tleh še ne pomeni, da nam bo na njem dejansko spodrsnilo (nevarnost). Tveganja in grožnje predstavljajo predpogoj za nevarnost, vendar pa to še ne pomeni dejanske nevarnosti.*

izvedbo tradicionalnih kaznivih dejanj do današnjih sodobnih kompleksnih visoko tehnoloških dejanj, izvedenih v celoti v kibernetskem prostoru. Definicije so tako dokaj splošne in poskušajo zajeti čim širši krog dejanj, ki bi jih lahko uvrstili v okvir kibernetske kriminalitete. Komisija evropskih skupnosti kibernetsko kriminaliteto opredeli dokaj ozko, in sicer kot »kazniva dejanja, storjena z uporabo elektronskih komunikacijskih omrežij in informacijskih sistemov ali proti takšnim omrežjem in sistemom« (Komisija evropskih skupnosti, 2007). Veliko širšo definicijo pa postavita Bernik in Meško, ki kibernetsko kriminaliteto opredelita kot »uporabo informacijsko-komunikacijskih tehnologij za izvedbo kaznivih dejanj« (Bernik in Meško, 2011).

Problematika preprečevanja in pregona kibernetske kriminalitete je močno povezana z virtualnim vidikom kibernetskega prostora, ki vpliva na percepcijo posameznika z vidika »virtualizacije« dejanj, izvedenih v kibernetskem prostoru. Posledično posameznik problematike ne vidi kot ogrožajoče, vse dokler se posledice ne odrazijo v fizičnem svetu. Strah pred kriminaliteto lahko vpliva na delovanje posameznika v fizičnem svetu (Meško, Petrovec, Areh, Muratbegović in Rep, 2006), le-to pa ne pomeni, da posamezniki občutek varnosti/nevarnosti dejansko prenesejo tudi v virtualno okolje. Namreč, v kibernetskem prostoru vsakdo predstavlja potencialno žrtev[4], vprašanje pa je, ali posamezniki grožnje tudi dojemajo na takšen način in kako le-to vpliva na njihovo delovanje v kibernetskem prostoru. Raziskava Eurobarometra je sicer pokazala, da uporabnike interneta skrbi kibernetska varnost, in sicer je kar 74 % sodelujočih izrazilo mnenje, da se je tveganje, da postanejo žrtev kibernetske kriminalitete povečalo v zadnjem letu, toda hkrati pa več kot polovica Evropejcev ne izvede primerih ukrepov za zaščito pred kibernetskimi kaznivimi dejanji[5] (Evropska komisija, 2012). Študija poznavanja kibernetskih groženj in strahu pred kriminaliteto v Sloveniji pa je pokazala, da se manj kot polovica ljudi strinja s tem, da je lahko »žrtev kibernetske kriminalitete vsakdo, ki uporablja računalnik«, kar nakazuje na nizko stopnjo ozaveščenosti ter hkrati tudi na dejstvo, da se za računalnikom mnogi počutijo varne, saj menijo, da kibernetski prostor nima stika z realnostjo in je ločen od realnega dogajanja (Bernik in Meško, 2011).

Kibernetski prostor predstavlja virtualno globalno okolje, zaradi česar zagotovitev sodelovanja organizacij na mednarodni ravni, opredelitev enotnih definicij pojmov, skupnih pravil delovanja in vzpostavitev sistema najboljših praks igra pomembno vlogo v boju proti kibernetski kriminaliteti. Ključna rešitev nedvomno leži v prevenciji, ki se mora osredotočiti na najšibkejši člen – povprečnega uporabnika. Ozaveščanje posameznikov na vseh ravneh je tako ključnega pomena za uspešno preprečevanje, omejevanje in tudi pregon kibernetske kriminalitete[6].

4 *Evropska komisija v svojem poročilu izpostavlja, da je dnevno približno milijon ljudi žrtev kibernetske kriminalitete. Poleg tega raziskava, izvedena s strani Evropske komisije v letu 2011, ocenjuje strošek kibernetske kriminalitete na svetovni ravni na 85 do 291 milijard EUR (Evropska komisija, 2012).*

5 *V raziskavi je sodelovalo cca 27.000 ljudi iz vseh držav članic EU (Evropska komisija, 2012).*

6 *Na področju kibernetske kriminalitete organi pregona praviloma delujejo zgolj represivno, in sicer je več kot 90 % primerov kibernetske kriminalitete obravnavanih na podlagi prijave posameznika ali organizacije (United Nations Office on Drugs and Crime, 2013).*

2 OPIS UPORABLJENE METODE IN VZORCA

V okviru raziskave problematike kibernetske kriminalitete kot sodobne varnostne grožnje v povezavi z ozaveščenostjo in vedenjem posameznika v kibernetskem prostoru je bilo uporabljeno neeksperimentalno raziskovanje družboslovnih pojavov, in sicer je tehnika zbiranja podatkov temeljila na metodi snežne kepe z uporabo elektronske pošte in socialnih omrežij. Pri uporabi metode snežne kepe naključno izberemo določeno število anketirancev, ki vprašalnik nadalje posredujejo svojim znancem; na takšen način se količina anketirancev veča kot snežna kepa ter učinkovito proizvaja vzorčno strukturo (Malhotra, 2002). Raziskava je bila izvedena v obliki elektronskih anketnih vprašalnikov z uporabo spletnega portala KwikSurveys (http://www.kwiksurveys.com). Oblikovana sta bila identična anketna vprašalnika, in sicer v slovenskem in angleškem jeziku. Anketna vprašalnika sta bila posredovana izbranim znancem preko elektronske pošte in socialnega omrežja, ki so ga nadalje posredovali svojim stikom. Prvi vprašalnik (v slovenskem jeziku) je bil tako posredovan posameznikom, ki živijo in delujejo v Sloveniji, drugi vprašalnik (preveden v angleški jezik) pa je bil posredovan posameznikom, ki živijo in delujejo v ZDA. Prvi vprašalnik je bil na razpolago 9 dni – v tem času je nanj odgovorilo 123 anketirancev, od tega so bili trije vprašalniki nepopolni, zato niso bili uporabljeni pri analizi. Drugi vprašalnik je bil odprt 11 dni – v tem času je nanj odgovorilo 81 anketirancev, pri čemer je bil en vprašalnik nepopoln in prav tako ni bil uporabljen pri analizi. V raziskavi je torej sodelovalo 200 anketirancev, pri čemer jih 40 % spada v skupino posameznikov živečih in delujočih na območju ZDA in 60 % v skupino posameznikov živečih in delujočih na področju Slovenije.

Omejitve raziskave izhajajo iz načina zbiranja podatkov, saj ne gre za preprosti naključni vzorec, ter iz velikosti obravnavanega vzorca, zato je treba te omejitve upoštevati pri generalizaciji podatkov. Razlog za tovrstno anketiranje je v predpostavki, da smo želeli v anketo vključiti aktivne spletne uporabnike, le-te pa je najlažje doseči z uporabo informacijskih tehnologij. Populacija anketirancev je tako vključevala posameznike na področju Slovenije ter posameznike na področju ZDA, ki aktivno uporabljajo internet. Na podlagi slednjega smo predpostavljali, da imajo anketiranci osnovno poznavanje informacijsko-komunikacijskih tehnologij. Anketiranje je bilo izvedeno v maju 2013, sodelovanje v raziskavi je bilo prostovoljno in anonimno.

Namen raziskave je analizirati ozaveščenost in delovanje posameznika v kibernetskem prostoru glede na njihovo poznavanje in razumevanje pojava kibernetske kriminalitete, s tem povezano preventivno delovanje in odnos do organov pregona ter ugotoviti ključne razlike med vedenjem in delovanjem posameznikov v posamični državi (Slovenija in ZDA) ter podati možnosti za izboljšavo področne problematike v Sloveniji. Anketni vprašalnik, oblikovan na podlagi preučene literature in obstoječih raziskav, je poleg splošnih demografskih podatkov vključeval naslednje vsebinske sklope: delovanje v kibernetskem prostoru, poznavanja varne rabe interneta in pojava kibernetske kriminalitete ter vedenje posameznika ob srečanju s kibernetsko kriminaliteto.

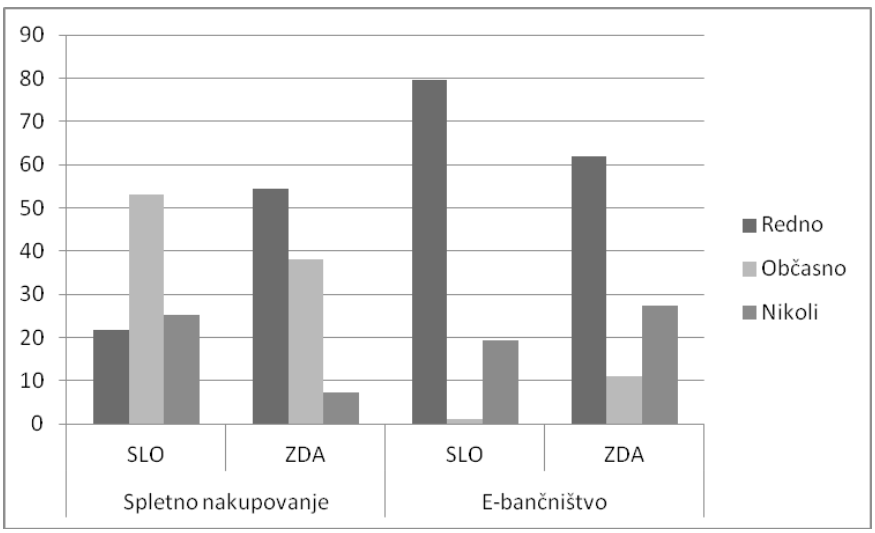
3 INTERPRETACIJA REZULTATOV RAZISKAVE

V nadaljevanju so prikazani rezultati analize zbranih podatkov, pri čemer smo se osredotočili na povezavo med znanjem oz. ozaveščenostjo, dejanskim vedenjem ter odnosom oz. percepcijo posameznika glede delovanja organov pregona na področju kibernetske kriminalitete v Sloveniji in ZDA. Analiza vključuje primerjavo med državama in povezavo na obravnavano problematiko pojavnosti, preprečevanja in pregona kibernetske kriminalitete.

3.1 Delovanje v kibernetskem prostoru

V okviru raziskave smo se najprej osredotočili na vprašanje delovanja posameznika v virtualnem prostoru, pri čemer nas je zanimala tako količina preživetega časa v kibernetskem prostoru kot tudi širina uporabljenih funkcionalnosti. V obeh skupinah anketirancev, torej tako skupini posameznikov, ki živijo in delujejo v Sloveniji (skupina SI), kot tudi skupini posameznikov, ki živijo in delujejo v ZDA (skupina ZDA), je količina časa preživetega v kibernetskem prostoru visoka, in sicer v obeh primerih cca 60 % anketirancev uporablja funkcionalnosti interneta več kot tri ure dnevno (skupina SI – 60 % in skupina ZDA – 66 %). Količina uporabe oz. preživetega časa v virtualnem okolju je torej v obeh skupinah primerljiva, nadalje pa nas je zanimalo, katere funkcionalnosti anketiranci uporabljajo.

Ena izmed najpogostejših oblik kibernetske kriminalitete je nedvomno kraja identitete, in sicer primarno kraja podatkov, povezanih z bančnimi računi (številke kreditnih kartic, dostopna gesla itd.), zato nas je najprej zanimalo, kako pogosto anketiranci uporabljajo spletne funkcionalnosti, ki vključujejo finančne prenose, in sicer smo se osredotočili na spletno nakupovanje z uporabo kreditne kartice in uporabo storitev e-bančništva (graf 1).



Graf 1: Spletne dejavnosti, povezane s finančnimi prenosi

V skupini SI največji odstotek (53 %) anketirancev izvaja nakupovanje preko spleta občasno[7], medtem ko največji delež anketirancev (55 %) skupine ZDA spletno nakupovanje izvaja redno[8]. Sklepamo, da gre v tem primeru za kulturne razlike in ne za odločitev, ki bi bila vezana na percepcijo večje ali manjše varnosti pri izvajanju spletnega nakupovanja. V nadaljevanju smo zato natančneje preučili povezavo med uporabo takšnih spletnih funkcionalnosti na eni strani ter poznavanjem pojavnih oblik kibernetske kriminalitete, občutkom lastne usposobljenosti glede spletne varnosti in občutkom varnosti v kibernetskem prostoru na drugi strani. E-bančništvo uporablja 81 % anketirancev skupine SI in 71 % anketirancev skupine ZDA, vendar pa je bistvena razlika v količini uporabe storitve, in sicer je pogostost uporabe e-bančništva višja v Sloveniji. V obeh primerih je uporaba e-bančništva široko razširjena, kar pripisujemo veliki stopnji zaupanja v varnost storitev, ki jih ponujajo bančne institucije.

Nadalje nas je zanimalo, ali je kakšna razlika v percepciji varnosti/nevarnosti kibernetskega okolja med obravnavanima skupinama, in sicer je raziskava pokazala, da imajo anketiranci v skupini SI močnejši občutek varnosti pri delovanju v kibernetskem prostoru, medtem ko se anketiranci v skupini ZDA čutijo bolj ogrožene, v okviru slednje skupine najvišji odstotek anketirancev meni, da kibernetski prostor ni preveč varen (57 %), medtem ko najvišji odstotek anketirancev v skupini SI meni, da je kibernetski prostor dokaj varen (39 %).

3.2 Poznavanje varne rabe informacijsko-komunikacijskih tehnologij in pojava kibernetske kriminalitete

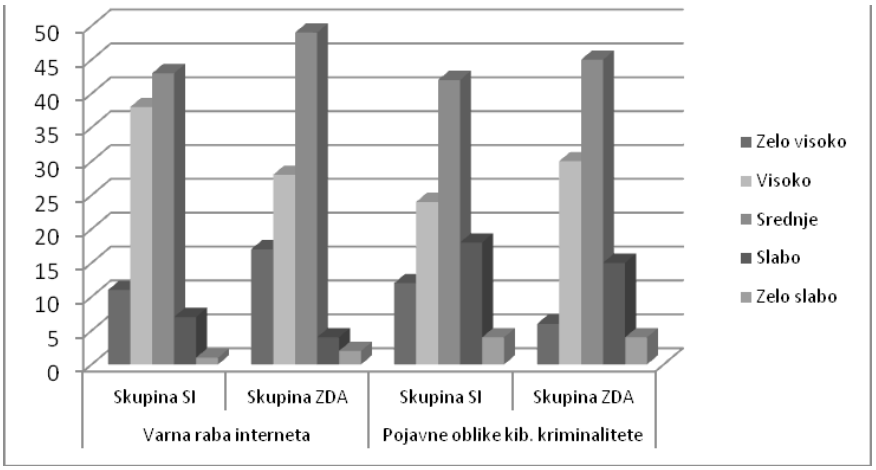
Kljub temu, da se jim kibernetski prostor na splošno ne zdi najbolj varen, anketiranci obeh skupin uporabljajo dokaj širok spekter funkcionalnosti, ki jih ponuja spletno okolje, zato nas je nadalje zanimalo, kako bi ocenili stopnjo svoje usposobljenosti na področju varne rabe informacijsko-komunikacijskih tehnologij ter stopnjo poznavanja pojava kibernetske kriminalitete v korelaciji s stopnjo uporabe funkcionalnosti, povezanih s finančnimi prenosi. Ob tem se zavedamo omejitve, povezane s problematiko definicije pojava kibernetske kriminalitete. V okviru raziskave smo se zato osredotočili na najširšo opredelitev, ki vključuje tako nove kot tudi tradicionalne oblike kriminalitete, ki so se prenesle v virtualno okolje.

Kot prikazano v grafu 2 se anketiranci v okviru obeh skupin v največji meri čutijo srednje usposobljene tako z vidika varne rabe interneta (43 % anketirancev skupine SI in 49 % anketirancev skupine ZDA) kakor tudi z vidika poznavanja pojavnih oblik kibernetske kriminalitete (42 % anketirancev skupine SI in 45 % anketirancev skupine ZDA).

Lastna ocena poznavanja/usposobljenosti je seveda lahko v veliki meri napačna, zato smo nadaljevali s konkretnimi vprašanji glede varnostnega ravnanja, in sicer smo se osredotočili na splošne oblike zagotavljanja varnosti, kot so nastavitve in menjava gesel ter varnostne nastavitve računalniškega sistema.

7 Nekajkrat letno

8 Vsaj nekajkrat mesečno



Graf 2: Ocena poznavanja/ usposobljenosti

Anketiranci obeh skupin so dokaj previdni v povezavi z uporabo gesel, in sicer jih velika večina uporablja različna gesla za različne storitve (npr. e-pošta, računalnik, socialno omrežje itd.); med anketiranci skupine SI kar 46 % sodelujočih uporablja drugačno geslo za vsako storitev, medtem je tako previdnih v skupini ZDA le 25 %, kjer največ anketirancev (57 %) sicer uporablja različna gesla, vendar pa ne drugačnega gesla za vsako storitev. Le 9 % anketirancev skupine SI uporablja isto geslo za vse storitve, medtem ko je ta odstotek v skupini anketirancev ZDA znatno višji, in sicer 19 %. Skupina anketirancev SI je torej bolj striktna glede uporabe različnih gesel, vendar pa varnostno delovanje žal odpove, ko se dotaknemo pogostosti menjave gesel, saj kar 50 % anketirancev skupine SI in 62 % anketirancev skupine ZDA gesla ne menjuje ali pa ga menja največ enkrat letno. Gesla je namreč priporočljivo redno menjati, sama pogostost menjave pa je odvisna od uporabljene storitve, za finančne storitve je tako priporočilo menjave gesla najmanj na dva meseca, ostala gesla pa na 3 do 4 mesece in ne redkeje kot na 6 mesecev (Granger, 2002).

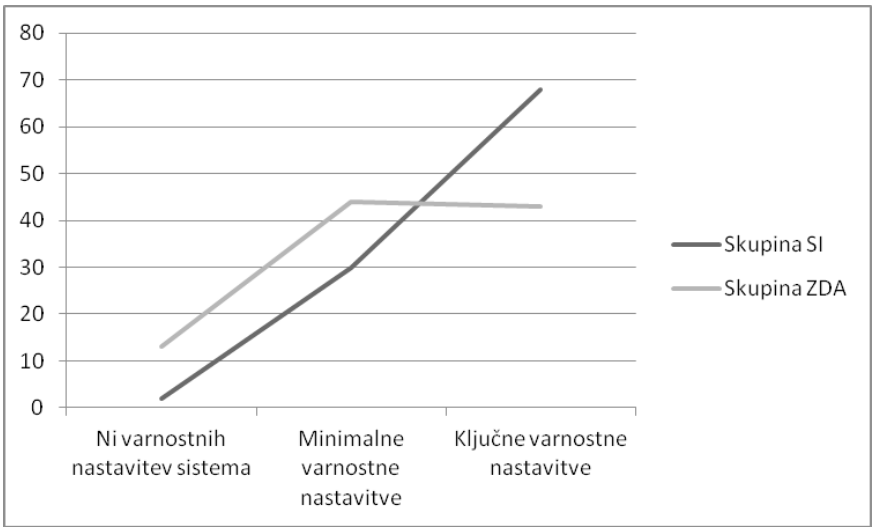
Z vidika varnostnih nastavitev računalniškega sistema smo anketirance povprašali, kakšne nastavitve imajo na lastnem sistemu oz. kako poskrbijo za varnost na svojem računalniku.

Kot prikazuje graf 3, so anketiranci skupine SI bolje poskrbeli za svoj računalniški sistem, saj velika večina (68 %) izvaja ključne aktivnosti za zagotovitev varnosti sistema (nameščen anti-virusni program, požarni zid, redno posodabljanje opreme itd.). Osnovnih varnostnih nastavitev sistema nima 2 % anketirancev skupine SI in 13 % anketirancev skupine ZDA. Pri tem je treba poudariti, da ni upoštevan tip uporabljene računalniške opreme glede na potencialne ranljivosti (npr. Apple).

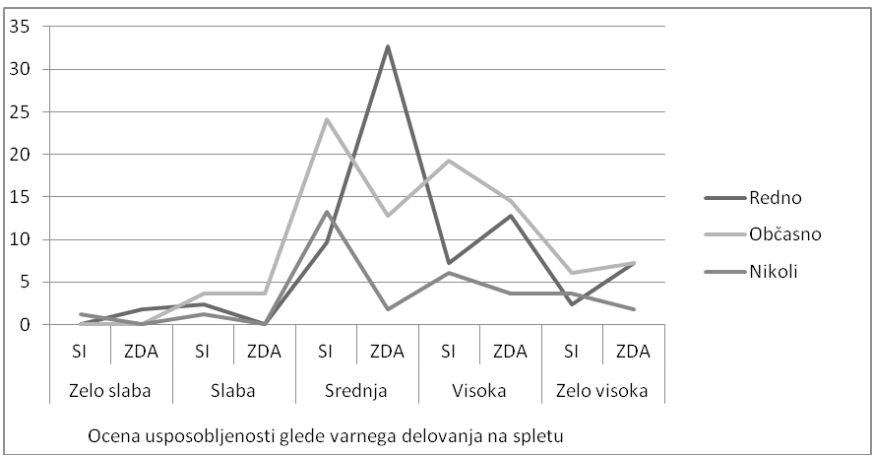
Glede na to, da je analiza pokazala dokaj visoko stopnjo zaupanja v storitve, ki jih ponujajo bančne institucije, smo se nadalje osredotočili na finančne prenose, povezane s spletnim nakupovanjem, v povezavi s čimer je opaziti porast primerov kibernetske kriminalitete v zadnjih letih. Zanimala nas je povezava med oceno stopnje usposobljenosti glede poznavanja varne rabe interneta in poznavanja

pojavnih oblik kibernetske kriminalitete na eni strani in stopnjo oz. pogostostjo izvajanja spletnih nakupov na drugi strani. Namreč, raziskava, izvedena v okviru EU, je pokazala, da »večina tistih, ki zaupajo spletnemu bančništvu in spletnemu nakupovanju, se počuti dobro obveščenih o kibernetski kriminaliteti« (Evropska komisija, 2012).

Graf 3: Varnostno ravnanje – nastavitve računalniškega sistema



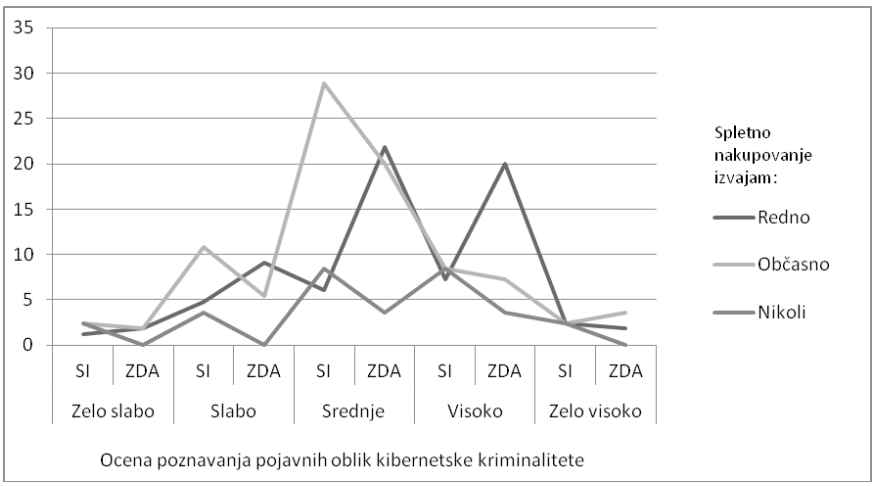
Graf 4: Uporaba funkcionalnosti spletnega nakupovanja v primerjavi z lastno oceno usposobljenosti glede varnega delovanja na spletu



Kot prikazuje graf 4, večina anketirancev skupine ZDA, ki redno uporablja funkcionalnosti spletnega nakupovanja z uporabo kreditne kartice, svojo usposobljenost glede varne rabe interneta ocenjuje kot srednje dobro, medtem ko v skupini SI najvišji odstotek tistih, ki redno uporablja takšno funkcionalnost, svojo usposobljenost ocenjuje kot visoko. Na splošno bi lahko v obeh primerih potrdili,

da se uporabniki, ki se odločijo za spletno nakupovanje, večinoma čutijo dovolj usposobljene tudi glede spletne varnosti.

V povezavi s poznavanjem pojavnih oblik kibernetske kriminalitete je analiza pokazala, da tako anketiranci skupine ZDA kot tudi anketiranci skupine SI, ki redno opravljajo spletne nakupe, svoje poznavanje pojavnih oblik kibernetske kriminalitete ocenjujejo kot srednje ali pa visoko (graf 5).



Graf 5: Uporaba funkcionalnosti spletnega nakupovanja v primerjavi z lastno oceno poznavanja pojavnih oblik kibernetske kriminalitete

Anketiranci v okviru obeh skupin ZDA in SI so torej v veliki meri prepričani v svojo usposobljenost glede varne rabe interneta in poznavanje pojavnih oblik kibernetske kriminalitete. Ob tem pa je zanimivo, da je večina anketirancev skupine ZDA, ki redno izvaja spletno nakupovanje (31 %), internet ocenila kot ne preveč varen, medtem ko je v skupini SI mnenje rednih spletnih nakupovalcev deljeno, in sicer med opcijama »ne preveč varen« (7 %) in »dokaj varen« (7 %).

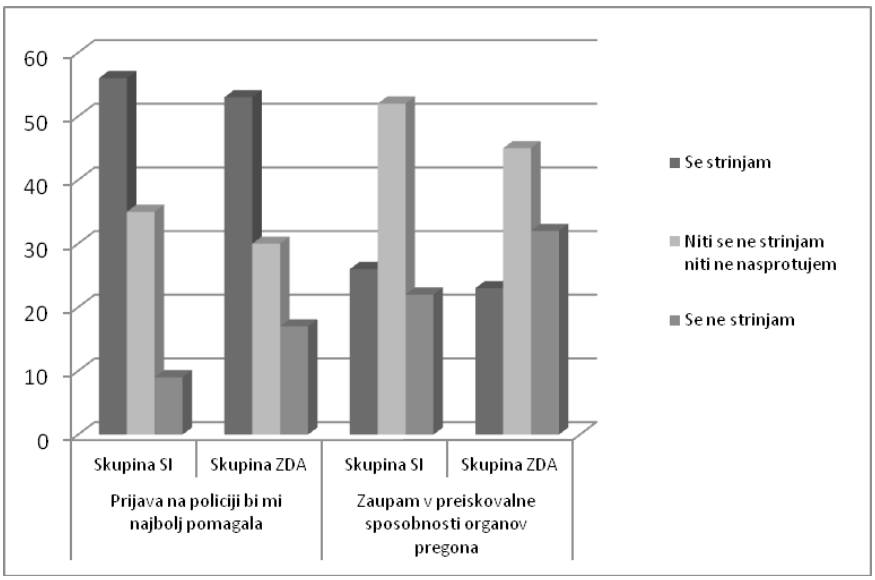
3.3 Vedenje posameznika ob srečanju s kibernetsko kriminaliteto

Uporaba funkcionalnosti informacijsko-komunikacijskih tehnologij nas spremlja na vseh področjih našega življenja in kot je pokazal prvi del raziskave, se anketiranci obeh skupin sicer zavedajo nevarnosti, pri čemer se bolj ogrožene počutijo anketiranci skupine ZDA, kar bi potencialno lahko pripisali manj varnemu fizičnemu okolju, hkrati pa do določene mere sicer delujejo varnostno, le-tega se bolj držijo anketiranci skupine SI, kar je zanimivo glede na dejstvo, da se anketiranci skupine ZDA počutijo bolj ogrožene, vendar pri svojem varnostnem ravnanju niso konsistentni. Obe skupini anketirancev pa se zavedata potencialnih posledic delovanja v virtualnem prostoru na fizični svet (v obeh skupinah več kot 80 % anketirancev meni, da dejanja v virtualnem okolju vplivajo na fizični svet).

Glede na to, da se anketiranci zavedajo potencialnih posledic virtualnega delovanja v fizičnem okolju, nas je nadalje zanimalo, kakšno bi bilo njihovo vedenje ob srečanju s kibernetsko kriminaliteto oz. s poskusom napada. Uporabili smo eno izmed najbolj razširjenih oblik poskusa kraja identitete, in sicer ribarjenje za podatki, pri čemer smo anketirancu predstavili situacijo, v kateri bi potencialno lahko postal tarča kraje identitete (prejeto elektronsko sporočilo z navodili za spremembo gesla s strani bančne institucije).

Večina anketirancev bi se uspešno obranila poskusa kraje identitete, še vedno pa se je bolj odrezala skupina SI, kjer bi se kar 92 % anketirancev pravilno odločilo in sporočila ne bi upoštevali oz. bi stopili v stik z odgovorno osebo, v skupini ZDA bi tako ravnalo 83 % anketirancev. Kraja identitete je zaradi finančnih posledic takšnega kaznivega dejanja v zadnjih letih pogosto obravnavana v medijih, zato takšen rezultat ni presenetljiv.

Nadalje nas je zanimalo, kakšen odnos oz. mnenje imajo anketiranci v povezavi z delovanjem organov pregona na področju kibernetske kriminalitete, in sicer smo se najprej osredotočili zgolj na prvi stik, torej prijavo kaznivega dejanja kibernetske kriminalitete. Večina udeležencev obeh skupin (več kot 50 % tako v skupini SI kot tudi v skupini ZDA) je mnenja, da bi ob srečanju s primerom kibernetske kriminalitete najbolj pomagala prijava na policiji, medtem ko jih tretjina ni prepričanih v učinek prijave. Večji problem predstavlja zaupanje v preiskovalne sposobnosti organov pregona, saj večina anketirancev ni vanje prepričana (približno polovica anketirancev v obeh skupinah), medtem ko slaba tretjina anketirancev v obeh skupinah ne zaupa preiskovalnim sposobnostim organov pregona (prikazano v grafu 6).



Graf 6: Odnos do organov pregona

4 RAZPRAVA

Skupaj z že omenjeno hitro rastjo števila uporabnikov sodobnih informacijsko-komunikacijskih tehnologij ne rasteta samo količina in popularnost ponujenih funkcionalnosti[9] (Kende, 2012), temveč tudi količina in raznolikost izvedenih dejanj kibernetske kriminalitete[10]. Predstavljena raziskava je pokazala primerljivo količino uporabe oz. preživetega časa v kibernetskem prostoru v obeh obravnavanih skupinah ter tudi široko uporabo ponujenih spletnih funkcionalnosti.

V povezavi z uporabo spletnih funkcionalnosti za izvajanje finančnih prenosov je na eni strani uporaba storitev, ki jih ponujajo kredibilne institucije (banke), široko razširjena v obeh skupinah, kar bi lahko pripisali veliki stopnji zaupanja v varnost storitev, ki jih takšne institucije ponujajo. Na drugi strani pa smo ugotovili, da se skupina SI še vedno bolj zanaša na fizični svet, medtem ko skupina ZDA preferira funkcionalnosti v celoti izvedene v kibernetskem prostoru, v kolikor se le-teh poslužuje. Seveda ob tem ne gre pozabiti, da storilci pogosto izrabljajo ravno zaupanje posameznika v kredibilnost in varnost poznane institucije (npr. PayPal) za izvedbo najrazličnejših zavajanj in prevar[11], zato je pomembno, da uporabniki prepoznajo potencialna tveganja in se pravilno odločajo ob srečanju z različnimi oblikami kibernetske kriminalitete.

Ena izmed najpogostejših oblik kibernetske kriminalitete je nedvomno kraja identitete, in sicer primarno kraja podatkov, povezanih z bančnimi računi (številke kreditnih kartic, dostopna gesla itd.), ki je tudi najbolj obravnavana v medijih, zato je bilo pričakovano, da se bodo ob podanem primeru poskusa napada ribarjenja za podatki udeleženci pravilno odločili, kar je raziskava tudi potrdila v okviru obeh obravnavanih skupin. Rezultat je v tem primeru skladen z ugotovitvijo, da se uporabniki, ki se odločijo za spletno nakupovanje, večinoma čutijo dovolj usposobljene tudi glede spletne varnosti in glede poznavanja pojavnih oblik kibernetske kriminalitete. Seveda pa takšne ugotovitve ne moremo posploševati na druge oblike kibernetske kriminalitete.

Glede na to, da so rezultati skupine ZDA na splošno pokazali širšo in bolj liberalno uporabo spletnih funkcionalnosti, lahko rezultat razlagamo na dva načina, in sicer, da se je skupina ZDA v virtualnem okolju preprosto udomačila, zaradi česar jih prisotnost potencialne nevarnosti ne ovira pri njihovem delovanju, ali pa lahko upoštevamo kulturne razlike in hitrost življenja, zaradi katere je uporaba informacijsko-komunikacijskih tehnologij neizogibna. Kulturne razlike po našem mnenju do določene mere vplivajo na količino uporabe funkcionalnosti informacijsko-komunikacijskih tehnologij, kar bi bilo smiselno dodatno preučiti v

9 *Julija 2010 je bila na primer naložena prva slika na takrat novo funkcionalnost – Instagram, dve leti kasneje je število naloženih slik naraslo na milijardo, ki jih je naložilo 50 milijonov uporabnikov (Kende, 2012).*

10 *Raziskava, izvedena leta 2012 v 24 državah sveta, ugotavlja, da je dnevno viktimiziranih kar 1,5 milijona posameznikov, pri čemer finančna škoda, povezana s kibernetsko kriminaliteto, znaša 110 milijarde USD na letni ravni (Symantec, 2012).*

11 *Eden izmed bolj popularnih načinov je ribarjenje za podatki (phishing), pri čemer storilci izrabijo zaupanje žrtve v kredibilen videz poslane pošte, da pridobijo želene podatke za nadaljnje zlorabe. V letu 2012 se je število takšnih napadov na svetovnem nivoju povečalo kar za 59 % v primerjavi z letom 2011 (RSA Security, 2012).*

nadaljnji raziskavi področja. Percepcijo varnosti pa lahko povežemo tudi s fizičnim okoljem življenja in delovanja v manjši oz. večji državi. Ljudje smo namreč fizična bitja in virtualno okolje na neki način še vedno predstavlja neznanko, zato se pravila fizičnega sveta v veliki meri poskušajo preslikati v virtualni svet. Prebivalci Slovenije se v svojem fizičnem okolju praviloma počutijo varnejše kot prebivalci ZDA, kar prenesejo tudi v virtualno okolje. Ob tem je zanimiva tudi visoka stopnja občutka usposobljenosti glede varne rabe interneta v okviru skupine SI, kjer se kar 49 % anketirancev čuti visoko ali zelo visoko usposobljene. Le-to bi potencialno lahko pripisali veliki količini ozaveščanja, izvedenega v zadnjem letu, ki se je osredotočalo primarno na potencialne zlorabe, povezane s finančnimi posledicami (npr. kraja identitete, prevare itd.)[12]. Ob tem pa je zanimivo dejstvo, da tako preprosta zaščita, kot je uporaba varnih gesel in njihova redna menjava, še vedno ni ukoreninjena v delovanje posameznika, saj velik del udeležencev[13] gesel ne menjuje redno (več kot enkrat letno). Raziskava je torej pokazala pomembno razliko med ozaveščenostjo posameznikov in njihovim dejanskim varnostnim ravnanjem v virtualnem okolju, ki pa se v osnovi ne razlikuje glede na fizično lokacijo posameznika.

V povezavi z delovanjem organov pregona na področju kibernetske kriminalitete je raziskava pokazala, da bi večina udeležencev sicer potencialno podala prijavo organom pregona, vendar pa večina v njihovo delovanje ni prepričana, kar je potrdilo ugotovitve drugih raziskav glede problematike zaupanja v preiskovalne sposobnosti organov pregona na področju kibernetske kriminalitete. Raziskava Urada Združenih narodov za droge in kriminal je tako pokazala, da velik del posameznikov na svetovnem nivoju ne prijavi primerov kibernetske kriminalitete, med glavne razloge med drugim spada tudi nizka stopnja zaupanja splošne javnosti v sposobnosti predstavnikov organov pregona (United Nations Office on Drugs and Crime, 2013). Ključnega pomena je torej, poleg aktivnosti, usmerjenih k ozaveščanju splošne javnosti glede problematike kibernetske kriminalitete in načinov varne rabe interneta, tudi ozaveščanje splošne javnosti glede pomena prijave kaznivih dejanj kibernetske kriminalitete in predvsem povečanje zaupanja v delovanje organov pregona tudi na področju visoko tehnoloških kaznivih dejanj.

Nivo znanja v kombinaciji z vedenjem posameznika predstavljata ključni dimenziji človeškega dejavnika v povezavi z zagotavljanjem informacijske varnosti in le z združitvijo obeh dimenzij je mogoče doseči visoko raven informacijske varnostne kulture (van Niekerk in von Solms, 2006). Podobno kot predstavljena raziskava namreč tudi druge raziskave kažejo občutno razliko med poznavanjem informacijskih groženj oz. stopnjo ozaveščenosti in dejanskim ukrepanjem; v zadnjih letih se je sicer izboljšalo razumevanje varnostnega vedenja – prva dimenzija, ni pa se spremenilo tudi varnostno vedenje posameznika – druga dimenzija (Rančigaj in Lobnikar, 2012). Slednje je potrdila tudi raziskava percepcije kibernetske kriminalitete v Sloveniji, ki je pokazala, da so, zaradi svoje virtualne narave in široke pojavnosti, določena dejanja, ki spadajo v okvir kibernetske kriminalitete, videna

12 *V letu 2011 je bil sprejet nacionalni program ozaveščanja o informacijski varnosti, ki ga izvaja Arnes s strokovno podporo SI-CERT v sodelovanju z Ministrstvom za izobraževanje, znanost in šport.*

13 *50 % skupine SI in 62 % skupine ZDA.*

kot sprejemljiva[14]. Ob tem je treba poudariti, da sta zaznavanje in interpretacija varnosti v veliki meri odvisna od splošne varnostne kulture; ko začne skupina kot celota moralno in socialno percipirati varnostne kršitve kot nesprejemljive in se posledično začne tudi varnostno obnašati, pride do prehoda od splošnega varnostnega zavedanja v varnostno kulturo (Lobnikar, Čaleta, Žaberl, Anžič in Rančigaj, 2009).

V okviru raziskave smo tako ugotovili, da so anketiranci precej samozavestni glede lastne usposobljenosti oz. poznavanja varne rabe interneta, vendar pa hkrati njihovo varnostno ravnanje ni zadostno predvsem z vidika konsistentnosti varne rabe. Pri tem naletimo na že prepoznano problematiko razlike med poznavanjem in dejanskim delovanjem v smislu »vem kako, a ne delam tako« (Rančigaj in Lobnikar, 2012), kar kaže na še vedno prenizko stopnjo informacijske varnostne kulture na področju uporabe funkcionalnosti informacijsko-komunikacijskih tehnologij v kibernetskem prostoru. Pomembno vlogo pri preprečevanju in omejevanju kibernetske kriminalitete namreč nedvomno odigra posameznik s svojim varnostnim ravnanjem v kibernetskem prostoru. Višjo stopnjo varnostnega ravnanja posameznika pa dosežemo z večjo ozaveščenostjo in poznavanjem oblik potencialnih napadov ter primernih odzivov/reakcij ob srečanju s kibernetsko kriminaliteto.

5 ZAKLJUČEK

Informacijsko-komunikacijske tehnologije predstavljajo nepogrešljiv del vsakdanjega življenja in delovanja, vendar pa se ob hitrem razvoju funkcionalnosti in razširjenosti kibernetskega prostora razumevanje in vedenje splošne javnosti nista primerno prilagodili. Kljub temu, da je nivo znanja oz. poznavanja pravil varne rabe interneta zadovoljiv, se le-to še vedno ne odrazi v varnostnem ravnanju posameznika v virtualnem okolju, kar je pokazala tudi predstavljena raziskava, saj že tako osnovno varnostno ravnanje, kot je redna menjava gesla, v veliki meri odpove. Problematičen je torej razkorak med ozaveščenostjo posameznikov in njihovim dejanskim varnostnim ravnanjem v virtualnem okolju, ki pa se v osnovi ne razlikuje glede na fizično lokacijo posameznika. Kljub temu se v povezavi z občutkom varnosti fizična lokacija dejansko preslika v virtualno okolje, saj so anketiranci živeči in delujoči v manjši državi (Slovenija) izrazili višjo stopnjo občutka varnosti v virtualnem okolju kot anketiranci živeči in delujoči v večji državi (Združene države Amerike). Dejstvo, da občutek varnosti bistveno ne vpliva na delovanje posameznika v kibernetskem prostoru, bi lahko pripisali virtualnemu vidiku kibernetskega prostora. V nadaljnjih raziskavah bi bilo zanimivo nadalje raziskati vpliv virtualnega vidika kibernetskega prostora tudi na vprašanje problematike percepcije viktimizacije, saj se, zlasti v primerih, kjer ni neposrednih finančnih posledic, velik del žrtev niti ne zaveda, da so bile

14 *Raziskava percepcije kibernetske kriminalitete je pokazala, da kar 65 % intervjuvancev razlikuje dejanje, izvedeno v virtualnem okolju, od dejanja, izvedenega v fizičnem svetu, pri čemer je večina mnenja, da je piratstvo programske opreme, filmov in glasbe družbeno sprejemljivo (Dimc in Dobovšek, 2010).*

izpostavljene kibernetski kriminaliteti (United Nations Office on Drugs and Crime, 2013). V povezavi z delovanjem organov pregona je problematičen predvsem skepticizem, povezan s percepcijo usposobljenosti predstavnikov organov pregona na področju kibernetske kriminalitete, in sicer je kar 75 % anketirancev izrazilo dvom v tehnično usposobljenost organov pregona. Slednje se potencialno lahko odraža v številu in verjetnosti prijave kaznivega dejanja kibernetske kriminalitete. Z vidika ozaveščanja splošne javnosti s ciljem dosega visokega nivoja varnostnega ravnanja bi bilo potrebno povečati količino aktivnosti, povezanih z ozaveščanjem, pri čemer bi se morali posvetiti tudi aktivnostim, ki bi zviševale stopnjo zaupanja v delovanje organov pregona. Le-ti bi morali preseči delovanje na represivni ravni in se usmeriti tudi v strateško obravnavo kaznivih dejanj kibernetske kriminalitete. Za vzpostavitev visokega nivoja varnostnega ravnanja posameznika v virtualnem okolju in posledično oblikovanje informacijske varnostne kulture na nacionalnem nivoju so ključnega pomena preventivne dejavnosti tako na nacionalnem kot tudi mednarodnem nivoju z namenom spremembe percepcije varnostnih kršitev v kibernetskem okolju in posledičnim povečanim varnostnim obnašanjem posameznika, s čimer bi presegli pozicijo »vem, vendar ne delam tako«[15].

LITERATURA

Bernik, I. in Meško, G. (2011). Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto. *Revija za kriminalistiko in kriminologijo, 62*(3), 242–252.

Britz, M. T. (2009). *Computer forensics and cyber crime*. New Jersey: Prentice Hall.

Dimc, M. (2009). Kriminaliteta v informacijski družbi. *Uporabna informatika, 17*(2), 101–105.

Dimc, M. in Dobovšek, B. (2010). Perception of cyber crime in Slovenia. *Varstvoslovje, 12*(4), 378–396.

Dlamini, M. T., Eloff, J. H. P. in Eloff, M. M. (2009). Information security: The moving target. *Computers & Security*, *28*(3–4), 189–198.

Dunn, M. (2005). *A comparative analysis of cybersecurity initiatives worldwide.* Geneva: International Telecommunication Union. Pridobljeno na http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf

Evropska komisija. (2012). *Kibernetska kriminaliteta: državljane EU skrbi varnost osebnih podatkov in spletnih plačil.* Pridobljeno na http://europa.eu/rapid/press-release_IP-12-751_sl.htm

Flaker, V. (1994). Analiza tveganja. *Socialno delo*, *33*(3), 189–196.

Gordon, S. in Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology and Hacking Techniques*, 2(1), 13–20.

15 *Posamezniki so namreč pogosto seznanjeni z osnovnimi varnostnimi tehnikami, vendar jih preprosto ne implementirajo (npr. uporaba varnih gesel, redna menjava gesel itd.).*

Granger, S. (2002). *The simplest security: A guide to better password practices*. Pridobljeno na http://www.symantec.com/connect/articles/simplest-security-guide-better-password-practices

Hundley, R. O., Anderson, R. H., Bikson, T. K., Botterman, M., Cave, J., Neu, C. R. et al. (2007). *RAND: The future of the information revolution in Europe: Proceedings of an international conference*. Pridobljeno na http://www.rand.org/content/dam/rand/pubs/conf_proceedings/2007/CF172.pdf

Internet Crime Complaint Center. (2008). *2008 internet crime report*. Pridobljeno na http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf

Internet Crime Complaint Center. (2012). *2012 internet crime report*. Pridobljeno na http://www.ic3.gov/media/annualreport/2012_IC3Report.pdf

Kende, M. (2012). *How the Internet continues to sustain growth and innovation*. Pridobljeno na http://www.internetsociety.org/sites/default/files/How%20the%20Internet%20continues%20to%20sustain%20growth%20and%20innovation.pdf

Komisija evropskih skupnosti. (2007). *Delovni dokument služb Komisije - Spremni dokument k sporočilo Komisije Evropskemu parlamentu, Svetu in Evropskemu odboru regij - Na poti k splošni politiki o boju proti kibernetskemu kriminalu*. Pridobljeno na http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007SC0641:SL:NOT

Kopetz, H. (2011). *Real-time systems*. New York: Springer.

Kovačič, M., Modic, D., Rusjan, M., Selinšek, L., Šavnik, J. in Završnik, A. (2010). *Kriminaliteta in tehnologija: kako računalniki spreminjajo nadzor in zasebnost, ter kriminaliteto in kazenski pregon.* Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti.

Lobnikar, B., Prislan, K., Markelj, B. in Banutai, E. (2012). Informacijskovarnostna ozaveščenost v javnem in zasebnem sektorju v Sloveniji. *Varstvoslovje, 14*(3), 345–363.

Lobnikar, B., Čaleta, D., Žaberl, M., Anžič, A. in Rančigaj, K. (2009). *Varnostna in organizacijska kultura v Slovenski vojski z vidika upravljanja s tajnimi podatki: končno poročilo raziskovalne skupine Fakultete za varnostne vede*. Ljubljana: Fakulteta za varnostne vede.

Malhotra, N. K. (2002). *Basic marketing research*. Upper Saddle River: Prentice Hall.

Markelj, B. in Bernik, I. (2011). Kombinirane grožnje informacijski varnosti pri rabi mobilnih naprav. V *Nove razmere in priložnosti v informatiki kot posledica družbenih sprememb, 18. Konferenca Dnevi slovenske informatike.* Ljubljana: Slovensko društvo Informatika.

Meško, G., Petrovec, D., Areh, I., Muratbegović, E. in Rep, M. (2006). Strah pred kriminaliteto – izzivi za raziskovanje. *Revija za kriminalistiko in kriminologijo, 49*(4), 346–353.

Miniwatts Marketing Group. (2013). *InternetWorldStats: Usage and population statistics*. Pridobljeno na http://www.internetworldstats.com/stats.htm

van Niekerk, J. in von Solms, R. (2006). *Understanding information security culture: A conceptual framework.* Johanesburg: Information Security South Africa. Pridobljeno na http://icsa.cs.up.ac.za/issa/2006/Proceedings/Full/21_Paper.pdf

Rančigaj, K. (2010). *Informacijska varnostna kultura v državni upravi* (Magistrsko delo). Ljubljana: Fakulteta za družbene vede.

Rančigaj, K. in Lobnikar, B. (2012). Vedenjski vidiki zagotavljanja informacijske varnosti. V I. Bernik in G. Meško (ur.), *Konferenca Informacijska varnost: odgovori na sodobne izzive, zbornik prispevkov.* Pridobljeno na http://www.fvv.uni-mb.si/konferencaIV/zbornik/Rancigaj_Lobnikar.pdf

RSA Security. (2012). *The year in phishing*. Pridobljeno na http://www.emc.com/collateral/fraud-report/online-rsa-fraud-report-012013.pdf

Shea, V. (2004). *Netiquette*. Pridobljeno na http://www.albion.com/netiquette/corerules.html

SI-CERT. (2012). *Nevarnost je odvisna od naše varnosti: Poročilo o omrežni varnosti za leto 2012*. Pridobljeno na https://www.cert.si/fileadmin/slike/si-cert/fokus/2013/SI-CERT_porocilo_2012.pdf

Raba interneta v Sloveniji. (2011). *Dostop do interneta ima 72 % slovenskih gospodinjstev*. Pridobljeno na http://www.ris.org/db/27/12187/Raziskave/Dostop_do_interneta_ima_72_slovenskih_gospodinjstev/?&p1=276&p2=285&p3=1318&db=160

Suler, J. (2004). The online disinhibition effect. *Cyber Psychology and Behavior, 7*(3), 321–326. Pridobljeno na http://www.samblackman.org/Articles/Suler.pdf

Svete, U. (2005). *Varnost v informacijski družbi*. Ljubljana: Fakulteta za družbene vede.

Symantec. (2012). *2012 Norton cybercrime report*. Pridobljeno na http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

Taylor, R. W., Caeti, T. J., Loper, K., Fritsch, E. J. in Liederbach, J. L. (2006). *Digital crime and digital terrorism*. New Jersey: Prentice Hall.

United Nations Office on Drugs and Crime. (2013). *Comprehensive study on cybercrime.* Pridobljeno na http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Cambridge: Polity Press.

O avtorjih:

Mag. Maja Dimc, predavateljica na področju kibernetske kriminalitete in informacijske varnosti, zaposlena na Ministrstvu za obrambo Republike Slovenije. E-mail: maja.dimc@gmail.com

Dr. Bojan Dobovšek, izredni profesor in prodekan na Fakulteti za varnostne vede Univerze v Mariboru. E-mail: bojan.dobovsek@fvv.uni-mb.si