Revija za kriminalistiko in kriminologijo / Ljubljana 67 / 2016 / 1, 44–60

Kibernetska korporativna varnost mobilnih naprav: zavedanje uporabnikov v Sloveniji

Blaž Markelj[1], **Aleš Završnik**[2]

Mobilne naprave so postale osrednje sodobno vozlišče informacijsko-komunikacijske tehnologije, saj poleg telefoniranja vključujejo številne funkcionalnosti in storitve. Skladno s tem se zato povečuje pomen posameznikovega zaznavanja in razumevanja njihove varne rabe. Z nepoznavanjem tveganj mobilnih naprav se povečuje tudi tveganje za sisteme in podatke organizacij, do katerih uporabniki dostopajo z mobilnimi napravami in na svojih napravah tudi shranjujejo njihove podatke.

V prvem delu članek opredeli osnovne pojme, pojem kibernetske ali informacijske varnosti, pojem varnosti omrežij in informacij (VOI) in pojem kibernetske kriminalitete. Pri tem pokaže nove usmeritve pri zakonodajnem urejanju VOI na evropski ravni in statistične trende, ki kažejo na veliko penetracijo mobilnih naprav v poslovnih (korporativnih) sistemih. Z namenom prikazati načine posameznikovega ravnanja z mobilno napravo, njegovo poznavanje groženj in odnosa do naprav, v drugem delu članek predstavi raziskavo o poznavanju groženj, stopnji tveganega vedenja pri uporabi mobilnih naprav in uporabi tehničnih zaščit zaposlenih v slovenskih organizacijah.

Ključne besede: kibernetska varnost, mobilne naprave, korporativna varnost, kibernetska kriminaliteta, varnost omrežij in informacij (VOI)

UDK: 004.056

1 Uvod

Tehnološki napredek pri pametnih telefonih, tablicah, nosljivem računalništvu (angl. *wearable computing*) in drugih brezžično povezanih napravah, kot so POS terminali (Kovacs, 2015), vodi v vedno večje deleže kibernetske kriminalitete in povečuje tveganja kibernetske varnosti. Stalna 24/7 povezanost teh naprav, raznovrstni načini dostopanja do omrežnih povezav, večja tveganja pred izgubo naprave ali odtujitvijo (primernejše tarče), spremenjena lastništva v sistemu »Prinesi svojo napravo« (angl. »*Bring-Your-Own-Device*«, BYOD), ki povečujejo varnostne grožnje in odtekanje informacij, so dejavniki, ki mobilne naprave postavljajo v ospredje kibernetske varnosti. Na primer Kaspersky Lab (2015a) poroča, da se je z odtekanjem informacij spopadlo že 17 odstotkov gospodarskih družb, ki so v sistem dela implementirale BYOD; v tipičnem primeru se to zgodi po prenehanju delovnega razmerja v organizaciji. Mobilne naprave, ki združujejo vse več tehnologij in aplikacij, postajajo vsenavzočne. V Sloveniji imamo že več let več naročnikov in predplačnikov mobilnega omrežja kot prebivalcev (na primer 2.326.000 uporabnikov mobilnega omrežja v 4. četrtletju 2014 (SURS, 2015)).

Statistika o tem, koliko uporabniki dostopajo do interneta »*on-the-go*«, kaže, da postajajo mobilne naprave ključne tarče kibernetskih napadov. Po podatkih SURS (2016) vedno več uporabnikov interneta dostopa do interneta, medtem ko so zunaj doma ali delovnega mesta (»*on-the-go*«). V Sloveniji je v prvem četrtletju leta 2015 kar 47 odstotkov uporabnikov interneta (starih 16–74 let) dostopalo do interneta tudi zunaj doma ali delovnega mesta in pri tem za dostop do interneta uporabljalo mobilni telefon (v letu 2014 je bilo takih uporabnikov interneta manj, 37 odstotkov). Od teh jih je večina, 91 odstotkov, dostopala do interneta prek mobilnih telefonskih omrežij, 68 odstotkov pa prek brezžičnega omrežja (Wi-Fi) (SURS, 2016), kar kaže na večji pomen na ranljivost obeh tipov omrežij.

Podatki za korporacijske rabe mobilnih naprav kažejo še večji porast uporabe mobilnih naprav. V raziskavi *IT Spending Priorities Survey 2012*, v kateri je sodelovalo 453 strokovnjakov IT, so ugotovili, da se organizacije zelo zanimajo za vlaganja v mobilne naprave (Feldman, 2012). Študija Kaspersky Lab (2015b) je pokazala, da kar dve tretjini (62 odstotkov) podjetij in njihovih zaposlenih uporablja osebne mobilne naprave za delo, kar pomeni, da BYOD ni več razvijajoči trend, ampak široko sprejeta poslovna praksa. Pri tem ugotavljajo, da 36 od-

[1] Dr. Blaž Markelj, predavatelj za informacijsko varnost, Fakulteta za varnostne vede Univerze v Mariboru, Slovenija. E-pošta: blaz.markelj@fvv.uni-mb.si

[2] Dr. Aleš Završnik, višji znanstveni sodelavec, Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani, in izredni profesor za kriminologijo, Pravna fakulteta Univerze v Ljubljani, Slovenija. E-pošta: ales.zavrsnik@pf.uni-lj.si

stotkov respondentov shranjuje na te naprave delovne dokumente, 34 odstotkov jih hrani z delom povezano elektronsko pošto. Včasih shranjujejo celo bolj zaupne podatke na svoje naprave, kot so gesla za dostop do službene e-pošte (18 odstotkov) in celo do navideznih zasebnih omrežij (VPN) (11 odstotkov). Ob tem je samo 10 odstotkov teh uporabnikov resno zaskrbljenih za varnost podatkov organizacije (Kaspersky Lab, 2015a). Kibernetski varnostni priročnik Belgijske podružnice ISACA (Belgian Cyber Security Guide, 2014) navaja številne ranljivosti korporativnega BYOD sistema in med 10 obveznimi ukrepi na področju kibernetske varnosti našteva prav zagotovitev varnosti mobilnih naprav (na primer z močnimi gesli, s posodabljanjem operacijskega sistema in zaščitnih programov, z vzpostavitvijo postopkov obveščanja v organizaciji v primeru kraje/izgube naprave, z oddaljenim brisanjem podatkov itn. (Belgian Cyber Security Guide, 2014: 27)). Korporacijska raba mobilnih naprav je naraščajoč trend in s tem tudi pomembno korporacijsko varnostno tveganje. S tem namenom in ciljem članek predstavi definicije kibernetske varnosti in kibernetske kriminalitete, njuno medsebojno interakcijo nasploh in specifičnost pri rabi mobilnih naprav v korporativnih okoljih. Namen članka je raziskati uporabnikovo poznavanje kibernetske varnosti, v sklop katere sodi tudi poznavanje groženj in rabe varnostnih rešitev. Oboje kaže na uporabnikovo ignoranco možnosti uresničitve groženj (tveganj) in morebitnih posledic. V prvem delu zato članek definira kibernetsko varnost, kibernetsko kriminaliteto in informacijsko varnost z vidika rabe mobilnih naprav, medtem ko v drugem delu z različnimi statističnimi metodami obravnava postavljeno hipotezo (»Uporabniki mobilnih naprav *ignorirajo obstoj kibernetskih groženj*, zato se ne zavedajo *pomembnosti podatkov* na mobilni napravi in jih *ni strah* pred njihovo izgubo.«), ki jo v diskusiji poveže s predhodnim teoretičnim delom. Okvir prispevka predstavlja področje kibernetske varnosti in kibernetske kriminalitete in njuno medsebojno prekrivanje ter ločevanje na specifičnem področju mobilnih naprav v poslovnem okolju.

2 Kibernetska varnost in kibernetska kriminaliteta

Kibernetska varnost (angl. *cyber security*) je vsebinsko izjemno raznovrsten pojem. V ožjem pomenu se nanaša na varnost omrežij in informacij (VOI) pred tveganji in incidenti, ki niso nujno povezani s kriminaliteto.[3] *Tveganja* so v tem smislu okoliščine ali dogodki, ki imajo lahko negativen učinek na varnost.[4] *Incidenti* so okoliščine ali dogodki, ki imajo dejansko negativen učinek na varnost. Varnostne incidente lahko povzročijo človeške napake, tehnične okvare ali zlonamerni kibernetski napadi. *Kibernetska varnost v ožjem smislu* je zato širši pojem od kibernetske kriminalitete, saj zadnja obsega le dejanja, ki jih je mogoče pripisati delovanju ljudi, njen okvir pa določa kazenskopravni sistem izbrane države.[5]

Varnost v kontekstu VOI pomeni »zmožnost omrežja ali informacijskega sistema, da na dani ravni zaupanja prepreči naključne ali zlonamerne dogodke, ki ogrožajo razpoložljivost, avtentičnost, celovitost in zaupnost shranjenih ali prenesenih podatkov ali povezanih storitev, ki jih ponujajo ali so dostopne preko navedenih omrežij in informacijskih sistemov« (Evropska komisija, 2013b: 2. točka 3. člena).

Kibernetska varnost v ožjem smislu med državami članicami EU ni poenotena. Zakonodajno poenotenje bo prvič doseženo šele z Direktivo o ukrepih za zagotavljanje visoke skupne ravni varnosti omrežij in informacij v Uniji (v nadaljevanju Direktiva o VOI), katere predlog so decembra 2015 potrdili v odborih Evropskega parlamenta in Sveta EU (Evropska komisija, 2015). Namen prvega evropskega zakonodajnega akta o kibernetski varnosti je povečati zaupanje v spletno okolje in omogočiti nemoteno delovanje Evropskega enotnega digitalnega trga, kar bo doseženo s poenotenjem vseh 28 nacionalnih sistemov. Predlog direktive pojmuje kibernetsko varnost širše od kibernetske kriminalitete ne le vsebinsko (ker obsega še nesreče in nenamerne napade), temveč tudi personalno. Države članice EU bodo morale določiti ponudnike kritičnih informacijskih storitev, ki bodo morali zagotavljati posebno odpornost lastnih IT sistemov na kibernetske napade. Imeli bodo novo obveznost, ki naj

[3] Namesto pojma *kibernetska* varnost nekateri predpisi uporabljajo pojem *informacijska* varnost. Na primer Direktiva 2013/40/EU Evropskega parlamenta in Sveta z dne 12. avgusta 2013 o napadih na informacijske sisteme in nadomestitvi Okvirnega sklepa Sveta 2005/222/PNZ (v nadaljevanju Direktiva 2013/40/EU) (2013) je nadomestila pojem računalniški sistem s širšim pojmom informacijski sistem – od tod zagotavljanje *informacijske* varnosti. Pojma uporabljamo kot sinonima.

[4] Pojem *tveganja* se pogosto uporablja kot sinonim za *grožnje*. Predlog Direktive o ukrepih za zagotavljanje visoke skupne ravni varnosti omrežij in informacij v Uniji (v nadaljevanju Predlog Direktive o VOI) (Evropska komisija, 2013b) ustanavlja Skupino za odzivanje na računalniške *grožnje* (Evropska komisija, 2013b: 7. člen), ki je odgovorna za obvladovanje *incidentov* in *tveganj*. Hkrati pa Komisija utemeljuje sprejetje direktive z navedbo, da je pričakovan rezultat in učinek sprejetja direktive občutno izboljšanje varstva potrošnikov, podjetij in vlad EU pred *incidenti*, *grožnjami* in *tveganji* VOI (angl. *network and information security (NIS) incidents, threats and risks*). Za razliko od tveganj in incidentov predlog Direktive o VOI (Evropska komisija, 2013b) groženj nikjer ne definira.

[5] Kritična kriminologija šteje za kriminaliteto tudi dejanja, ki so škodna in ne nujno že inkriminirana. Vendarle je cilj kritičnih kriminologov preko kritike cone kriminalnega *de lege lata* doseči, da bi tudi takšna dejanja vstopila v cono kriminalnega *de lege ferenda* (Kanduč, 2015: 665).

prepreči dosedanje stanje zanikanja kibernetskih viktimizacij s tem, da bodo morali prijavljati resne varnostne vdore v njihove sisteme nacionalnim oblastem. Predlog Direktive VOI določa seznam tržnih udeležencev, ki imajo zaradi družbenega pomena posebne obveznosti na dva načina: 1) vse spletne dejavnosti, ki sodijo v eno izmed naslednjih kategorij: a) platforme za e--trgovanje, b) portale za spletna plačila, c) družbena omrežja, č) iskalniki, d) računalniške storitve v oblaku in e) prodajalne z aplikacijami (točka a 8. odstavka 3. člena, 2. točka 3. člena Predloga Direktive o VOI (Evropska komisija, 2013b)) z neizčrpnim navajanjem upravljavcev kritične infrastrukture na področjih energetike, prometa, bančništva, borze in zdravja (točka b. 8. odstavka 3. člena Predloga Direktive o VOI (Evropska komisija, 2013b)). Personalno gre za razširitev subjektov, saj to niso le podjetja, ki zagotavljajo javna elektronska komunikacijska omrežja (po Direktivi 2002/21/ES Evropskega parlamenta in Sveta z dne 7. marca 2002 o skupnem regulativnem okviru za elektronska komunikacijska omrežja in storitve (2002) (v nadaljevanju Direktiva 2002/21/ES), temveč so subjekti tudi izven sektorja elektronskih komunikacij (na primer na področju prometa in zdravja).

Druga novost, ki jo prinaša Direktiva o VOI, je, da bodo morale države članice EU ustanoviti posebne organe, če jih še nimajo, tj. skupine za odzivanje na računalniške grožnje (*Computer Security Incident Response Teams* – CSIRTs oziroma *Computer Emergency Response Teams* – CERTs), ki bodo odgovorni za obvladovanje kibernetskih varnostnih incidentov in tveganj, za čezmejno sodelovanje in usklajevanje skupnih odzivov na incidente. Sodelovanje med državami bo potekalo preko Mreže za sodelovanje in s pomočjo Evropske agencije za varnost omrežij in informacij (ENISA).

Kibernetsko varnost v širšem smislu lahko od kibernetske kriminalitete ločimo tudi glede na internetne plasti. Kibernetsko varnost lahko razumemo kot varnost (Doria, 2007): 1) internetnih protokolov, kjer gre za objekte varstva, za katere skrbi IETF (*Internet Engineering Task Force*), 2) varnost mreže, ki jo varujejo odzivni centri (CERTs), 3) varnost poslovanja na internetu, ki ščiti interese podjetij (na primer varnost e-bančnih storitev), 4) varnost državne suverenosti in nacionalnih interesov (na primer kibernetskega vojskovanja in kibernetskega terorizma) in 5) varnost posameznika oziroma njegovih temeljnih človekovih pravic in svoboščin (na primer informacijske zasebnosti).

Vse navedeno pomeni, da *kibernetska varnost v širšem pomenu* obsega tri osnovne stebre (Evropska komisija, 2013a: 17; Završnik, 2015: 18):

1) omrežno in informacijsko varnost (VOI), za katero v Sloveniji skrbi SI-CERT (Nacionalni odzivni center za obravnavo incidentov s področja VOI, ki opravlja tudi naloge vladnega centra za odzivanje na omrežne incidente in deluje v okviru javnega zavoda ARNES – Akademska in raziskovalna mreža Slovenije) oziroma imenovana tudi *kibernetska varnost v ožjem pomenu*;

2) varstvo pred *kibernetsko kriminaliteto*, ki sodi v domeno dejavnosti organov odkrivanja in pregona kaznivih dejanj in

3) *kibernetsko vojskovanje*, tj. aktivnosti obrambnih sil, za katero so v Sloveniji zadolžene enote za elektronsko bojevanje Slovenske vojske (prim. Zakon o obrambi, 2004: 32. člen).

Korporativna (poslovna) varnost (angl. *corporate security*) v informacijski družbi zaradi digitalizacije poslovnih procesov gospodarskih in drugih subjektov neizogibno vključuje tudi kibernetsko varnostne vidike. Korporativna varnost je sistem za zagotavljanje notranje varnosti podjetja in obsega celoto pravnih, organizacijskih, funkcionalnih, tehničnih in kadrovskih ukrepov v skrbi za ohranitev reda, spoštovanje zakonov in internih predpisov ter varnost ljudi in premoženja v podjetju (Čaleta, Rančigaj in Lobnikar, 2011; Gostič, 2008). To je dejavnost, katere namen je identificirati in izvesti vse potrebne sistemske ukrepe za obvladovanje varnostnih tveganj v posamezni organizaciji in predstavlja eno od funkcij korporacije (Čaleta in Čaleta 2012: 107). Zavedanje uporabnikov je zato prvi pogoj za boj s kibernetskimi grožnjami, tveganji in incidenti z mobilnimi napravami, ki so uporabljane v poslovne namene.

3 Raziskovanje zavedanja uporabnikov o tveganjih z mobilnimi napravami

V skladu z naraščajočo rabo mobilnih naprav, ki jo potrjujejo raziskave o rabi, naraščajo tudi *grožnje* mobilnim napravam. To so najhitreje razvijajoče se informacijske grožnje prihodnosti (Olavsrud, 2013). Grožnje uporabnikom mobilnih naprav posredno ali neposredno ogrožajo tudi informacijske sisteme organizacij in organizacije, če kompromitirana mobilna naprava deluje tudi znotraj njih ali če sta mobilna naprava in informacijski sistem organizacije povezana (Markelj, 2014). Skrb za varnost je zato odvisna od *zavedanja* o nevarnostnih in tveganjih, ki je prvi člen pri celovitem zagotavljanju varnosti. Šele zavedanje (vednost) skupaj s primernim odnosom (motivacijo) in obnašanjem lahko zagotavlja kibernetsko varnost (glej t. i. KAB (angl. *knowledge-attitude-behaviour*) teorijo, Lobnikar, Prislan, Markelj in Banutai (2012: 352)).

V raziskavi o zavedanju groženj informacijski varnosti strokovnjakov za IKT, ki so na takšnih položajih, da odločajo o zagotavljanju in vzdrževanju informacijske varnosti, Chicone (2009) ugotavlja, da se uporabniki v poslovnem svetu vedno bolj zavedajo tovrstnih groženj. Raziskava, ki jo je

izvedla, je bila namenjena pregledu pomanjkljivosti (v varnostnem smislu) pri uporabi mobilnih naprav v ameriških zasebnih in javnih podjetjih ter organizacijah.

Obstoječe raziskave o zavedanju kibernetskih groženj v *Sloveniji* kažejo, da obstaja »splošno pomanjkanje ozaveščenosti o kibernetski kriminaliteti in kibernetski zakonodaji med ljudmi, ki stalno uporabljajo informacijsko-komunikacijske tehnologije za službene in zasebne namene« (Bernik in Meško, 2011: 250). »Kljub znanju uporabnikov pri uporabi računalniških orodij in delu v kibernetskem prostoru zavedanje na področju informacijske varnosti relativno majhno.« (Bernik in Meško, 2011: 248). Rezultati raziskave kažejo, da uporabniki bolj poznajo medijsko izpostavljene grožnje, kakor pa tiste, pred katerimi bi se dejansko morali zaščititi. Bernik in Meško (2011) še ugotavljata, da se vprašani z višjo stopnjo izobrazbe in/ali višjo starostjo manj bojijo kibernetske kriminalitete, kar je posledica boljšega znanja in izkušenosti ter na podlagi tega višje stopnje ozaveščenosti in boljše zaščite računalnika z elementarnimi programi in orodji za zaščito (Bernik in Meško, 2011: 249). Završnik in Levičnik (2014) pri preverjanju odnosa do zasebnosti in ukrepanju posameznikov, da bi varovali svojo zasebnost, ugotavljata, da so deleži zavedanja groženj (zasebnosti) visoki, a so respondenti hkrati nemotivirani ukrepati na podlagi tega znanja. Sčasoma z naraščanjem uporabe mobilnih naprav se zavest o grožnjah nujno ne povečuje. Na primer razmerje med poznavanjem groženj mobilnim napravam v letih 2011 in 2015 ni naraslo v vseh vidikih. Pešić (2015) ugotavlja, da se je med fizičnimi (ne korporativnimi) uporabniki zavedanje o nekaterih posamičnih grožnjah sicer povečalo, a se je v celoti zavedanje o grožnjah mobilnim napravam v letu 2015 v primerjavi z letom 2011 zmanjšalo (Pešić, 2015: 10–12, 37). Raziskava med študentsko populacijo o rabi mobilnih naprav, ki sta jo izvedla Bernik in Markelj (2014), je v zvezi z zavedanjem pokazala, da vprašani poznajo predvsem grožnje iz obdobja osebnih računalnikov, medtem ko je poznavanje groženj, ki so vezane na mobilne naprave, pretežno slabo.

Teorija v odgovor na grožnje ponuja večnivojske *ukrepe* (Herath in Rao, 2009). Informacijska varnost pri upravljanju s tveganji ne pomeni le uvajanja tehničnih rešitev, temveč se je treba osredotočiti na socialno-tehnične in psiho-socialne vidike zagotavljanja kibernetske varnosti. Pomembna je organizacijska varnostna *kultura* (Lobnikar et al., 2012), ki vsebuje 10 elementov (Lobnikar et al., 2012; OECD, 2002: 9–12). Del te kulture je *organizacijska dinamika* kot »najpomembnejši dejavnik, ki vpliva na procese ponotranjenja pravil varnostnega vedenja in vedenjske vplive zaposlenih« (Čaleta et al., 2011). Podobno poudarjajo Kury, Meško, Mitar in Fields (2009), ki vidijo organizacijsko kulturo kot ključen dejavnik, ki vpliva na vedenje ljudi v nekem okolju.

4 Raziskava o celoviti rabi mobilnih naprav v organizacijah

4.1 Metoda

Za namene ugotavljanja celovite rabe mobilnih naprav v organizacijskih okoljih smo izvedli raziskavo s pomočjo spletnega vprašalnika, ki je bil v času od maja 2012 do februarja 2013 objavljen na spletnem portalu »1ka« (www.1ka.si). Na vprašalnik je v tem času odgovorilo nekaj več kot 600 uporabnikov mobilnih naprav iz 34 različnih organizacij v Sloveniji. Skoraj polovica vprašalnikov je bila izpolnjena nepopolno – te smo izločili iz nadaljnje analize in za statistično obdelavo uporabili *309 vprašalnikov*.

4.1.1 Struktura vprašalnika

Vprašalnik je vseboval vprašanja zaprtega tipa. Sestavili smo ga na podlagi pregleda literature o informacijski varnosti mobilnih naprav (Brodkin 2008; Juniper Networks, 2010, 2011a, 2011b; Lookout 2011; McAfee, 2011, 2012). Vprašalnik smo pred tem preizkusili na osmih naključno izbranih uporabnikih mobilnih naprav, zaposlenih v organizacijah, sodelujočih v naši raziskavi. Težav z razumevanjem trditev v vprašalniku ni bilo, zato smo vprašalnik pustili nespremenjen. S prvim delom vprašalnika (5 vprašanj) smo pridobili demografske podatke organizacij in anketiranih ljudi (velikost podjetja, sektor, primarna dejavnost organizacije, dosežena stopnja izobrazbe anketiranca). V drugem delu vprašalnika (15 vprašanj) so se vprašanja in postavljene trditve nanašali na ugotavljanje stanja na področju varnosti uporabe mobilnih naprav. Zanesljivost merjenja vprašalnika (tistega sklopa, ki ga obravnavamo za namene tega članka) smo preverjali s Chronbach alfa, ki je 0,853).

4.1.2 Vzorec

Na podlagi pridobljenih podatkov iz Statističnega urada Republike Slovenije (SURS, 2014) smo izmed 314.059 podjetij naključno izbrali 50 podjetij. V vzorec prvega dela raziskave (anketiranec) smo vključili vse redno zaposlene v različnih organizacijah v Sloveniji, ki so uporabniki mobilnih naprav. Izvedba raziskave je temeljila na pošiljanju dostopa do elektronske ankete (povezave) s spremnim dopisom kontaktni osebi v posamezni organizaciji. V dopisu smo kontaktno osebo v posamezni organizaciji seznanili s področjem raziskovanja in pojasnili svoj namen. Sledila sta telefonski pogovor in osebni sestanek. Zaradi občutljivosti tematike raziskave in velike zaposlenosti v sodelovanje niso privolile vse organizacije, temveč 34 organizacij. Kontaktna oseba v posamezni organizaciji je pozneje sama posredovala povezavo zaposlenim, ki so izpolnjevali vprašalnik prostovoljno po svoji presoji in anonimno.

4.1.3 Uporabljene statistične metode

Pridobljene podatke v raziskavi smo analizirali z orodjem SPSS. Za analizo osnovnih demografskih podatkov smo uporabili izračune deležev, medtem ko smo za statistično obravnavo (zavrnitev ali nezavrnitev) hipoteze – predstavljene v nadaljevanju – uporabili:

– *Klaster analizo* oziroma analizo razvrščanja (združevanja) v skupine, s katero smo respondente glede na vprašanje »Pri rabi mobilnih naprav se mi lahko zgodi« (tabela 1) razvrstili v skupine, ki smo jih uporabili v nadaljevanju članka pri dveh drugih vprašanjih, ponovno za potrebe preverjanja postavljene hipoteze;

– test enakosti skupin (ANOVA), s katerim smo potrdili utemeljenost odločitve deljenja respondentov na tri skupine (tabela 2);

– izračun aritmetične sredine, kar smo uporabili za dodelitev imen posameznim predhodno oblikovanim skupinam (slika 1);

– diskriminantno analizo (Stepwise), Wilksovo lambdo in Fisherjevo linearno diskriminantno analizo, ki smo jih uporabili za določanja vpliva posameznih spremenljivk (groženj) na posamezno skupino in med skupinami (tabela 3, 4 in 5).

4.2 Raziskava

4.2.1 Demografski podatki respondentov

Osnovni podatki o respondentih so obsegali vprašanja o velikosti organizacije, iz katere respondenti prihajajo (81 odstotkov iz velikih podjetij, 2 odstotka iz mikropodjetij, 8 odstotkov iz majhnih podjetij in 9 odstotkov iz srednje velikih podjetij); takšno razmerje pripisujemo temu, da je v večjih podjetjih odgovarjalo na anketo več ljudi. Glede na stopnjo izobrazbe respondentov jih je največ, 65 odstotkov, končalo višjo, visoko ali univerzitetno stopnjo študija, 19 odstotkov srednješolski program, 15 odstotkov jih je imelo magisterij ali doktorat. Iz navedenega sklepamo, da ima velika večina respondentov stopnjo izobrazbe, ki jim (teoretično) omogoča dovolj visoko stopnjo razgledanosti, da bi lahko:

– prepoznali *grožnje* mobilnim napravam,
– pomen *posledic* ob uresničitvi groženj in
– pomen *rabe varnostne zaščite.*

4.2.2 Hipoteza

Z analizo rezultatov spletne ankete smo preverili veljavnost naslednje hipoteze:

H1: »Uporabniki mobilnih naprav *ignorirajo obstoj kibernetskih groženj*, zato se ne zavedajo *pomembnosti podatkov* na mobilni napravi in jih *ni strah* pred njihovo izgubo.«

Če se vprašani zavedajo groženj, hkrati pa imajo na mobilni napravi podatke, ki so za organizacijo in posameznika pomembni in ne uporabljajo ustreznih varnostnih rešitev, sklepamo, da namenoma ignorirajo obstoj kibernetskih groženj in pred izgubo podatkov ne občutijo nobenega strahu.

Na podlagi danih spremenljivk pri vprašanju o poznavanju in zavedanju groženj smo oblikovali skupine vprašanih, ki se glede na spremenljivke najbolj razlikujejo med seboj. Tako smo odgovorili na vprašanje, *koliko se posamezna skupina vprašanih zaveda in boji* groženj. Zatem smo ugotovili, *katere vsebine* imajo te skupine na mobilni napravi ter *katere varnostne rešitve* uporabljajo.

Za preverjanje hipoteze smo uporabili statistične analize podatkov, pridobljenih iz treh vprašanj:

1) »Pri rabi mobilnih napravi se mi lahko zgodi«;
2) »Vrste vsebine, shranjene na mobilni napravi«;
3) »Vrste uporabljenih zaščit«.

4.2.3 Uporabnikovo zavedanje groženj

Seznam devetih groženj, vključenih v vprašalnik, temelji na doslejšnjih raziskavah o grožnjah (Bernik, 2014; Markelj, 2014: 44–50; Norton, 2012; OWASP, 2013; Varni na internetu, 2013; WEB-Center, 2012). Rezultati odgovorov na *vprašanje o poznavanju in zavedanju groženj*, ki pretijo uporabnikom mobilnih naprav (tabela 1), predstavljajo osnovo za oblikovanje skupin (po Markelj, 2014: 95–98). Šele na podlagi analize podatkov o odgovorih na vprašanje »Pri rabi mobilnih naprav se mi lahko zgodi« smo ustvarili sliko o tem, koliko vprašani poznajo in se zavedajo groženj.

Tabela 1: Pri rabi mobilnih naprav se mi lahko zgodi

	1 – Grožnje ne poznam	2 – Ne verjamem	3 – Verjamem	4 – Se mi je že zgodilo
Odtujitev mobilne naprave	2 %	7 %	83 %	8 %
Kraja podatkov	3 %	10 %	86 %	1 %
Vdor prek Bluetootha	8 %	27 %	65 %	0 %
Sledenje (posledica nenadzorovanega oddajanja GPS-modula)	6 %	19 %	74 %	1 %
Prevzem nadzora nad mobilno napravo	9 %	23 %	68 %	0 %
Oddajanje podatkov brez moje vednosti	6 %	16 %	76 %	2 %
Prestrezanje govorne komunikacije	6 %	14 %	80 %	0 %
Prestrezanje prenosa podatkov	6 %	13 %	81 %	0 %
Okužba z zlonamerno kodo (malware, spyware, virusi, trojanski konji itn.)	4 %	8 %	87 %	1 %

Tabela 1 torej prikazuje, koliko se vprašani zavedajo groženj uporabnikom mobilnih naprav. Vprašani so pri vsaki od naštetih groženj ovrednotili intenziteto poznavanja posamezne grožnje, in sicer od 1 (»Grožnje ne poznam«) do 4 (»Se mi je že zgodilo«). Iz rezultatov je razvidno, da je pri vsaki spremenljivki *prevladujoč delež tistih, ki verjamejo v grožnje*. To pomeni, da se respondenti zavedajo groženj, ki jim pretijo ob rabi mobilnih naprav, in jih torej poznajo. Razdelitev odgovorov od 1 (»Grožnje ne poznam«) do 4 (»Se mi je že zgodilo«) je relevantna tudi za nadaljnje preučevanje in razlage znotraj posameznih – v nadaljevanju oblikovanih – skupin.

Ker predvidevamo, da obstajajo skupine uporabnikov mobilnih naprav, ki imajo različen odnos do groženj, smo v nadaljevanju naredili *Klaster analizo* oziroma analizo razvrščanja (združevanja) v skupine. Skupine, ustvarjene pri tem vprašanju, smo uporabili pri nadaljnjih vprašanjih o vsebinah na mobilni napravi (glej 4.2.5 spodaj) in rabi varnostnih zaščit (glej 4.2.6 spodaj). Za oblikovanje skupin uporabnikov mobilnih naprav smo uporabili *Ward metodo,* ki ustvari skupine tako, da se skupine navzven čim bolj razlikujejo in da so navznoter čim bolj homogene.

Najbolj optimalno število skupin, da še zadovoljimo tema dvema kriterijema, je *tri*. To je mogoče dokazati še z analizo razlik med skupinami, tj. z *metodo diskriminantne analize*. Osnovni cilj diskriminantne analize je poiskati linearno kombinacijo merjenih spremenljivk, da bodo vnaprej določene skupine med seboj oziroma navzven čim bolj različne, napaka pri uvrščanju enot v posamezno skupino pa bo čim manjša. Pri diskriminantni analizi iščemo tiste razsežnosti podatkov, ki kar najbolj pojasnjujejo razlike med skupinami.

S *testom enakosti skupin* (tabela 2) smo potrdili utemeljenost odločitve deljenja respondentov na tri skupine. Ugotavljali smo, ali je naša odločitev o treh skupinah pravilna: ali se povprečne vrednosti dovolj razlikujejo med seboj glede na to, kateri skupini pripadajo.

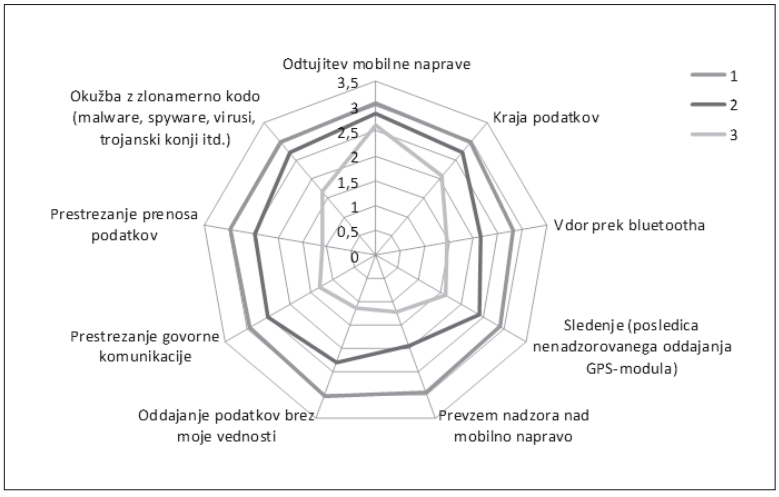
Tabela 2: Test enakosti skupin (ANOVA)

Spremenljivke	Skupina		Napaka		F	p
	Povprečje kvadratov	df	Povprečje kvadratov	df		
Odtujitev mobilne naprave	1,581	2	0,219	291	7,223	0,001
Kraja podatkov	7,718	2	0,149	285	51,834	0,000
Vdor prek bluetootha	21,462	2	0,259	285	83,011	0,000
Sledenje (posledica nenadzorovanega oddajanja GPS-modula)	15,750	2	0,236	287	66,674	0,000
Prevzem nadzora nad mobilno napravo	41,570	2	0,142	285	293,780	0,000
Oddajanje podatkov brez moje vednosti	30,160	2	0,142	283	213,137	0,000
Prestrezanje govorne komunikacije	20,747	2	0,171	288	121,464	0,000
Prestrezanje prenosa podatkov	27,948	2	0,113	285	248,104	0,000
Okužba z zlonamerno kodo (malware, spyware, virusi, trojanski konji itd.)	12,678	2	0,135	286	93,846	0,000

(df – stopnja prostosti, p – vrednost)

Stopnja statistične značilnost (p - vrednost) vseh testov je pod 0,05, zato ničelno hipotezo o enakosti skupin zavrnemo in sprejmemo nasprotno. Sklepamo, da so razlike med skupinami za vse spremenljivke statistično značilne, kar potrjuje pravilnost izbire treh skupin.

V nadaljevanju smo prej oblikovanim trem skupinam določili predznak: katera je tista skupina respondentov, ki v grožnje »*verjame*« (ta nas glede na postavljeno hipotezo najbolj zanima), katera je tista, ki v grožnje »*ne verjame, ne pozna*«, in katera je skupina neodločenih uporabnikov mobilnih naprav (»*verjame/ne verjame*«). Te podatke je mogoče razbrati iz polarnega grafa (slika 1).



Slika 1: Polarni graf

Še bolj nazorno je mogoče tovrstno razporeditev v tri posamezne skupine prikazati s polarnim grafom (slika 1). Skupine so razvrščene po vrstnem redu po številu članov: skupina označena s številko ena predstavlja skupino ljudi, ki je najbolj številna (199 respondentov) in ima aritmetično vrednosti pri posameznih grožnjah okoli vrednosti 3 (*skupina »verjamem«*). Druga skupina, ki šteje 81 vprašanih, označena s številko 2, ima aritmetično vrednost posameznih groženj med 2 in 3, zato lahko rečemo, da v to skupino sodijo respondenti, ki se ne morejo odločiti, ali naj verjamejo v resnost groženj ali ne (*neodločena skupina*). Najmanj številčna skupina, v polarnem grafu označena s številko 3 (14 respondentov), ima večino vrednosti aritmetičnih sredin posameznih groženj med 1 in 2 (med odgovoroma *»ne poznam in ne verjamem«*). Ta skupina *»ne verjamem«* najmanj verjame v resnost groženj, malo bolj se respondenti te skupine bojijo le odtujitve mobilne naprave.

Po doslej uporabljenih statističnih metodah se tako kaže odločitev o obstoju treh skupin respondentov glede poznavanja in zavedanja groženj pravilna. Na podlagi izračuna povprečnih vrednosti smo jih poimenovali in umestili. Katere pa so tiste *spremenljivke, ki najbolj ločujejo posamezne skupine*? Te spremenljivke pokažejo, katere grožnje najbolj vplivajo na vprašane uporabnike mobilnih naprav (in vplivajo na njihovo umestitev v predhodno oblikovane skupine).

Spremenljivke smo iskali z diskriminantno analizo, kjer smo se odločili za *hierarhično metodo* (STEPVISE). Značilnost te metode je, da izbere tiste spremenljivke, ki najbolj ločujejo skupine. V naslednji tabeli (tabela 3) je razvidno, da so prišle v izbor samo grožnje, pri katerih je raznolikost med skupinami dovolj velika (izpadla je grožnja »odtujitev mobilne naprave«).

Ta metoda je izpostavila – tako znotraj skupin kot med skupinami – spremenljivke (v našem primeru je to nabor groženj), ki najbolj vplivajo na skupino oz. imajo največji vpliv (tabela 3). Tako smo v nadaljevanju lahko ugotovili, katera je tista grožnja, ki ima največji vpliv znotraj skupine, ki v grožnje verjame, ter največji vpliv med vsemi tremi skupinami.

Z namenom potrditi, da so spremenljivke v tabeli 4 resnično tiste, ki prispevajo k ločevanju predhodno postavljenih skupin, smo naredili še izračun Wilksove Lambde (tabela 4).

Tabela 3: Seznam spremenljivk (groženj) za nadaljnjo analizo (vključevanje posamezne spremenljivke v Fisherjevo diskriminantno funkcijo)

Spremenljivke	F	Wilksova Lambda
Prevzem nadzora nad mobilno napravo	74,839	0,143
Prestrezanje prenosa podatkov	35,629	0,116
Oddajanje podatkov brez moje vednosti	20,573	0,106
Vdor prek bluetootha	14,505	0,102
Okužba z zlonamerno kodo (malware, spyware, virusi, trojanski konji itd.)	12,335	0,100
Prestrezanje govorne komunikacije	8,440	0,097
Sledenje (posledica nenadzorovanega oddajanja GPS-modula)	5,392	0,095

Tabela 4: Wilksova Lambda

Število spremenljivk	Lambda	df[6]1	df2	df3	F			
					Statistics	df1	df2	p
1	0,307	1	2	275	310,386	2	275,000	0,000
2	0,147	2	2	275	220,376	4	548,000	0,000
3	0,127	3	2	275	164,027	6	546,000	0,000
4	0,111	4	2	275	136,266	8	544,000	0,000
5	0,103	5	2	275	115,034	10	542,000	0,000
6	0,095	6	2	275	100,742	12	540,000	0,000
7	0,092	7	2	275	88,500	14	538,000	0,000

(df – stopnja prostosti, p – vrednost)

Kot je iz tabele 4 razvidno, je statistična značilnost vseh linearnih kombinacij pod 0,05 (glej p), zato sklepamo, da vse prikazane spremenljivke značilno prispevajo k ločevanju prej omenjenih treh skupin. Wilksova Lambda torej potrjuje nabor groženj, med katerimi so razlike zadostne, da lahko ugotavljamo njihov vpliv znotraj posamezne skupine in med skupinami.

4.2.4 Analiza posamičnih groženj

Poleg povprečnih vrednosti znotraj posamezne skupine smo analizirali še posamične grožnje, in sicer smo poiskali, katera grožnja je najbolj pomembna oziroma katere se respondenti najbolj bojijo. Primerjali smo posamezne grožnje med skupinama in znotraj skupin.

Primerjavo smo izvedli s pomočjo Fisherjeve linearne diskriminantne analize. Za primerjavo smo uporabili tabelo diskriminantnih uteži: večja, kot je utež, večji je pomen te spremenljivke.

Tabela 5: Fisherjeva linearna diskriminantna analiza

	Skupine		
	1	2	3
Vdor prek bluetootha	10,503	7,383	4,833
Sledenje (posledica nenadzorovanega oddajanja GPS-modula)	11,852	10,416	6,919
Prevzem nadzora nad mobilno napravo	25,387	16,840	10,166
Oddajanje podatkov brez moje vednosti	19,873	15,655	7,694
Prestrezanje govorne komunikacije	14,335	11,828	6,824
Prestrezanje prenosa podatkov	27,772	22,077	9,460
Okužba z zlonamerno kodo (malware, spyware, virusi, trojanski konji itd.)	19,491	18,384	11,745

[6] Stopnja prostosti

Iz tabele 5 je razvidno, da ima v skupini »verjamem« (skupina 1) največji vpliv grožnja *prestrezanja prenosa podatkov* (27,772), sledi ji *prevzem nadzora nad mobilno napravo* (25,387). Če se ti grožnji uresničita, lahko resno in težko posežeta v potek posameznikovega življenja, saj pride do kršitev pravice do posameznikove zasebnosti. Na primer prevzem nadzora nad mobilno napravo omogoča prestrezanje komunikacije (poseg v komunikacijsko zasebnost), analizo gibanja osebe preko lokacijskih podatkov (poseg v lokacijsko zasebnost), pregled slikovnega in drugega avdio in/ali video gradiva, shranjenega na mobilni napravi, poseg v osebnostne pravice in tudi razkritje občutljivih osebnih podatkov, ki so posebna kategorija osebnih podatkov (na primer veroizpoved). Ti grožnji lahko posežeta tudi v vitalne poslovne interese podjetja (na primer razkritje vsebine pogodb s poslovnimi partnerji, patentnimi prijavami in drugih poslovnih tajnosti). Hkrati sta obe omenjeni grožnji tudi tisti, ki imata največji razpon med tremi skupinami, torej se odgovori med posameznimi skupinami v zvezi s to grožnjo najbolj razlikujejo. To pomeni, da ima največji vpliv na vprašane in povzroča največji strah.

4.2.5 Shranjene vsebine na mobilni napravi

Oblikovanje skupin respondentov glede na njihovo poznavanje in zavedanje groženj mobilnim napravam in določitev posameznih spremenljivk (groženj), ki imajo največji vpliv znotraj skupin in med skupinami, smo primerjali z odgovori respondentov o *vsebinah*, ki jih shranjujejo na mobilni napravi (v nadaljevanju pod točko c), in tudi katero zaščito uporabljajo). Uporabili smo tri že oblikovane skupine, kar pomeni, da je maksimalno število vprašanih, razvrščenih v posamezne skupine, tudi v nadaljevanju ostalo enako. Vendar smo se osredotočili na najštevilčnejšo skupino »verjamem«, ker ta najbolj vpliva na potrjevanje postavljene hipoteze.

V tabeli 6 so predstavljene vsebine, ki jih imajo vprašani na mobilnih napravah, v korelaciji s tremi skupinami, sestavljenimi pri vprašanju o poznavanju groženj. Rezultati kažejo, kolikšno je število tistih, ki imajo na mobilni napravi podatke, ki so pomembni za organizacijsko in za osebno rabo, njihova izguba bi vplivala na delovanje osebe in organizacije ter so hkrati v posameznih predhodno definiranih skupinah. Iz tabele 7 je razvidno, da imajo respondenti iz skupine »verjamem« v grožnje, na mobilni napravi vsebine, ki bi ob uresničitvi grožnje lahko naredile *veliko škode*. Največji vpliv med grožnjami v skupini »verjamem« ima namreč grožnja prestrezanja podatkov, hkrati pa imajo respondenti v isti skupini na mobilni napravi seznam stikov (188 vprašanih), fotografije (174 vprašanih), službene dokumente (21 vprašanih) in dokumente z oznako tajno (5 vprašanih). Uresničitev prej omenjene grožnje bi povzročila prestrezanje prenosa teh podatkov in posledično razkritje vsebin tretjim osebam. Glede na to, da so v naboru vsebin tudi dokumenti z oznako tajno, certifikati, številke alarmnih sistemov itn., bi tovrstna uresničitev groženj povzročila resno škodo organizaciji in uporabniku. Zato bi bilo smiselno uporabiti ustrezne varnostne rešitve, da do uresničitve tovrstnih groženj sploh ne pride.

Tabela 6: Vsebine na mobilni napravi

Vsebina/Grožnje (skupine)	1[7]	2[8]	3[9]
	Število respondentov		
Seznam stikov	188	73	12
Fotografije	174	71	11
Domači elektronski naslovi	119	60	5
Zasebni koledar	124	50	8
Službena elektronska pošta	116	52	8
Službeni elektronski naslovi	115	30	6
Službeni koledar	114	49	6
Osebna elektronska pošta	112	54	3
Videovsebine	110	40	4
Domači naslovi	66	33	4
Službeni naslovi	58	29	4
Gesla (PIN-kode) za plačilne kartice	35	17	5
Službeni dokumenti	21	12	14
Certifikati (za banko, za dostop do poslovnih sistemov idr.)	11	3	2
Številke alarmnih sistemov	7	7	1
Gesla (PIN-kode) za mobilno bančništvo	7	6	1
Gesla za dostop do poslovnih sistemov	7	5	0
Dokumenti z oznako tajno	5	1	14

4.2.6 Raba varnostnih rešitev

Za preverjanje hipoteze smo respondente spraševali o uporabi varnostnih rešitev. Natančneje smo analizirali tisto skupino vprašanih, ki verjame v uresničitev groženj oziroma meni, da je tveganje veliko (Skupina *»verjamem«*).

[7] Skupina »verjamem«.

[8] Skupina neodločenih.

[9] Skupina »verjamem«.

Tabela 7: Varnostne rešitve na mobilni napravi glede na skupine poznavanja groženj

Varnostne rešitve/Grožnje (skupine)	1[10]		2[11]		3[12]	
	DA	NE	DA	NE	DA	NE
	Število respondentov					
Gesla ali PIN za dostop do mobilne naprave	173	21	66	13	13	1
Kriptiranje podatkov	40	*142*	17	60	4	9
Možnost oddaljenega brisanja vsebin mobilne naprave (v primeru odtujitve naprave)	51	136	26	63	3	9
Protivirusna zaščita	65	*121*	30	48	4	7
Zagotavljanje varne povezave mobilne naprave do informacijskega sistema organizacije (npr. VPN-povezava)	85	99	48	28	3	9
Sinhronizacija vsebin mobilne naprave	127	26	63	16	5	8
Centralni nadzor mobilne naprave (organizacija prek sistemov določi, kako lahko upravljam z mobilno napravo in katere funkcije lahko uporabljam)	40	145	25	51	4	8
Sledenje, SMS obveščanje idr., ki mi omogoča, da samostojno pridobim informacije o odtujeni/izgubljeni mobilni napravi	35	*151*	20	58	1	11
Znanje iz izobraževanj o funkcijah in varnosti mobilne naprave	96	90	41	36	5	7

V predhodnem podpoglavju smo pokazali, da imata znotraj skupine »verjamem« in med skupinami (ki smo jih predhodno določili) največji vpliv grožnji prestrezanje prenosa podatkov in prevzem nadzora nad mobilno napravo. Da se zavarujemo pred tovrstnima grožnjama, je treba uporabiti ustrezne varnostne rešitve, začenši s protivirusno zaščito, kriptiranjem podatkov, samostojnim sledenjem in morebitnim SMS obveščanjem v primeru kraje mobilne naprave. Vendar pa ugotavljamo, da uporabniki, ki verjamejo v uresničitev tovrstnih groženj (skupina »verjamem«) in imajo hkrati na mobilni napravi zelo pomembne podatke (tveganje pred izgubo podatkov je večje) (tabela 8, stolpec 1), ne uporabljajo zaščitnih varnostnih rešitev. Iz tabele 8 izhaja, da v skupini »verjamem« v grožnje samo 40 vprašanih (v skupini »verjamem« je 199 vprašanih, od tega se jih je do omenjene varnostne rešitve skupaj opredelilo 182 in samo 21,97 odstotka od teh to rešitev uporablja) uporablja kriptiranje na mobilni napravi, samo 35 vprašanih uporablja SMS obveščanje in samo dobra polovica uporablja protivirusno zaščito (tabela 7, v kurzivu).

Hipoteze pričujoče raziskave – »Uporabniki mobilnih naprav *ignorirajo obstoj kibernetskih groženj*, zato se ne zavedajo *pomembnosti podatkov* na mobilni napravi in jih *ni strah* pred njihovo izgubo.« – ni mogoče zavrniti. Iz predstavljenih rezultatov raziskave je razvidno, da uporabniki mobilnih naprav, ki so sodelovali v raziskavi, še posebej tisti, ki verjamejo v obstoj groženj, *kljub zavedanju o teh grožnjah* in zato tudi *pomembnosti podatkov* na njihovih mobilnih napravah, *ne uporabljajo zadostnih varnostnih rešitev*. Uporabniki mobilnih naprav se lahko zavedajo groženj, vendar ocenjujejo, da je uresničitev groženj majhna. Zaradi tega so stopnje strahu pred izgubo pomembnih (poslovnih in osebnih podatkov) na mobilni napravi majhne. V nasprotnem primeru bi uporabniki uporabljali ustrezne varnostne rešitve in bi zaradi potencialnih groženj zaščitili podatke na mobilni napravi.

[10] Skupina »verjamem«.

[11] Skupina neodločenih.

[12] Skupina »verjamem«.

5 Diskusija

V informacijski družbi, v kateri so podatki »novo gorivo«, pomen omreženih mobilnih naprav skokovito narašča. Mobilno (»*on-the-go*«) rabo povečuje ne le splošno prebivalstvo, temveč tudi poslovni subjekti, zaradi česar je tematika pomembna tudi z vidika korporativne (poslovne) varnosti. Preventivni programi v obliki izobraževanja uporabnikov so zato nujni. Ukrepi so številni in zato je treba integrirati v poslovne prakse že obstoječa in znana pravila, ki so jih pripravila različna strokovna združenja ali strokovnjaki, na primer o uporabi varnih gesel (IJS, 2016; Kovačič, 2012; Safe.si, 2016); o vzpostavitvi obveznosti uporabnikom uporabljati primerne varnostne nastavitve in posodabljati operacijski sistem vključno z zaščitnimi programi, o vzpostavitvi postopkov obveščanja znotraj organizacije v primeru kraje ali izgube naprave, z vnaprej predvideno možnostjo oddaljenega brisanja podatkov, s krepitvijo zavesti zaposlenih o previdnem pregledovanju naprav brez navzočih radovednih pogledov (Belgian Cyber Security Guide, 2014: 27).

Drugič, (samo)kritično o uporabnosti dodajamo, da se postopno spreminja pojem *mobilne naprave*, kar ima občutne posledice za kibernetsko korporativno varnost. Razvoj »interneta stvari« (*Internet of Things*, IoT) v pričujoči raziskavi še nismo dovolj zajeli. Pri IoT ne gre več samo za to, da mobilne naprave združujejo več tehnologij in aplikacij in s tem postajajo osrednje tarče kibernetskih napadov, nanje pa preži vedno več kibernetskih tveganj, tj. okoliščin ali dogodkov, ki imajo lahko negativen učinek na varnost. IoT številne predmete vsakodnevne rabe spreminja v IT naprave, povezane z internetom, kar pomeni, da bodo kibernetska tveganja in incidenti, povezani s predmeti, kot so hladilniki (Kanellos, 2016), (službeni) avtomobili (Newcomb, 2013), jedilni pribor (CES, 2016) ali pametni števci (Evropska komisija, 2014) v poslovnih prostorih. Na primer med zadnjimi so števci električne energije, pri katerih si je Evropska komisija postavila za cilj, da bo 80 odstotkov evropskih odjemalcev imelo do leta 2020 pametne električne števce (Skupni raziskovalni center Evropske komisije, 2014). Kibernetska varnost »mobilnih naprav« bo obsegala milijarde senzorjev, vgrajenih v različne predmete in naprave. Ti bodo omogočili opazovanje in komunikacijo s stavbami, avtomobili, delovnim okoljem, povezave predmetov z drugimi predmeti ali s posamezniki (t. i. *Wearable computing*), torej stvarmi, oblikovanimi tako, da snemajo, obdelujejo, shranjujejo ali posredujejo podatke. A te osnovne dejavnosti (zapisovanja, shranjevanja, obdelovanja in posredovanja podatkov) bodo postale pomembne tudi v luči temeljnih načel kibernetske varnosti: načela zaupnosti, integritete (podatkom ni nič odvzeto, dodano ali spremenjeno) in dostopnosti sistema in podatkov oziroma v luči načel C. I. A. (C – *confidentiality*, I – *integrity*, A – *availability*).

Delovna skupina iz člena 29[13] zato v mnenju št. 8/2014, ki se nanaša na tri vrste IoT mobilnih naprav (nosljivo računalništvo,[14] »kvantificirano sebstvo«[15] in hišna avtomatizacija[16]), utemeljeno opozarja na pomen kibernetske varnosti in zasebnosti pri »pametnih stvareh«. IoT ne prinaša izzivov le za varstvo zasebnosti, temveč prinaša velika varnostna tveganja za podatke zaradi slabe zaščite v napravah, v komunikacijskih povezavah in v shranjevalni infrastrukturi (Delovna skupina iz člena 29, 2014: 9). V mnenju Delovna skupina navaja negotovost pri tehtanju dvojnih nasprotnih teženj, ki jih morajo pomiriti proizvajalci IoT stvari: ukrepe, ki bodo implementirali zaupnost, integriteto in dostopnost na vseh ravneh obdelovanja podatkov, in potrebo po optimizirani uporabi računskih zmogljivosti naprave in njeno energetsko učinkovitostjo. Če tehtanje ne bo zadosti upoštevalo prvega, bo IoT spremenil vsakodnevne naprave, ki bodo razširile obstoječo različico interneta, v tarče informacijskih napadov. Manj varnostno zaščitene naprave namreč predstavljajo potencialno nove učinkovite načine za napade, olajšujejo nadzorstvene prakse, napade na informacijske sisteme in posledično kraje osebnih podatkov in drugo kompromitiranje podatkov, ki ima lahko velike učinke na pravice potrošnikov, dojemanje varnosti IoT in korporativno varnost. Naprave in platforme, povezane v IoT, bodo izmenjevale podatke in jih shranjevale na infrastrukturi ponudnikov storitev, zato bi morala biti kibernetska varnost IoT zasnovana ne le na napravah, temveč tudi na komunikacijskih povezavah, shranjevalni infrastrukturi in pri drugih vnosih v IoT ekosistem (prav tam).

---

[13] Delovna skupina za varstvo posameznikov pri obdelavi osebnih podatkov (krajše imenovana Delovna skupina iz člena 29) združuje vse predstavnike nadzornih organov za varstvo osebnih podatkov držav članic EU (v Sloveniji je to Informacijski pooblaščenec) je bila ustanovljena po Direktivi Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov.

[14] Nosljivo računalništvo (angl. *Wearable Computing*) se nanaša na vsakodnevne predmete in oblačila, kot so ure in očala, v katerih so senzorji za povečanje njihove funkcionalnosti (npr. Googlova očala s kamero, projekcijo sporočil idr. funkcionalnostmi pametnega telefona).

[15] Stvari paradigme »kvantificiranega sebstva« (angl. *Quantified Self*) so oblikovane tako, da jih lahko redno prenašajo posamezniki, ki želijo zapisovati podatke o lastnih navadah in življenjskem slogu. Primeri vključujejo naprave za zapisovanja gibanja, naprave, ki merijo in poročajo kvantitativne indikatorje posameznikovih fizičnih naporov, kot so porabljene kalorije, prehojeni koraki, srčni utrip in druge telesne znake. Glej še pojem *Lifelogging*.

[16] Hišna avtomatizacija ali »domotika« (angl. *domotics*) so IoT naprave, nameščene v pisarnah ali domovih v obliki na internet povezanih svetil, termostatov, detektorjev dima, vremenskih postaj, pralnih strojev ipd. naprav, ki jih je zaradi omreženosti mogoče upravljati na daljavo preko interneta. Na primer te naprave preko senzorjev zaznavajo prisotnost ali vzorce gibanja oseb in prilagodijo svojo prednastavljeno delovanje. Pogosto te podatke prenašajo nazaj k proizvajalcem.

Tretjič, kibernetska varnost bodisi fizičnih oseb bodisi pravnih (poslovnih) subjektov se pogosto zamenjuje s pojmom kibernetske kriminalitete. Za zadnji pojem velja, da je plod človekovih dejanj ali opustitev, medtem ko za kibernetsko varnost velja, da je lahko izgubljena tudi zaradi nesreč. Zaradi pogoste zamenljivosti pojmov smo zato v uvodu pojasnili osnovne razlike, posebej v luči sprejema evropske Direktive o zagotavljanju varnosti omrežij in informacij, ki bo prvič v zgodovini poenotila zagotavljanje kibernetske varnosti med državami članicami EU in predpisala nove obveznosti korporacijskim subjektom, katerih delovanje je temeljnega pomena za delovanje sodobnih »podatkovno razgaljenih družb« (Harcourt, 2015). Ker se prispevek ukvarja z varnostjo mobilnih naprav poslovnih subjektov (pravnih oseb), je treba zaradi digitalizacije njihovih poslovnih procesov neizogibno vključiti v varnostne ocene tudi kibernetskovarnostne vidike. Prva naloga oziroma prvi pogoj je zato analiza zavedanja o kibernetski varnosti mobilnih naprav, kar opravlja pričujoča raziskava.

Četrtič, zavedanje uporabnikov o kibernetskih tveganjih je bilo že predmet domačih raziskav, čeprav ne specifično za korporacijske rabe, temveč med splošno ali študentsko populacijo (Bernik in Meško, 2011; Bernik in Markelj, 2014; Pešić, 2015), specifično za varovanje zasebnosti (Završnik in Levičnik, 2014) ali za mobilne naprave (Bernik in Prislan, 2012), medtem ko je bilo opravljenih več raziskav v tujem okolju (Chicone 2015). Rezultati pričujoče raziskave potrjujejo ugotovitve, da je pri zagotavljanju kibernetske varnosti potreben vedenjsko-upravljavski pristop, da je pomembna organizacijsko-varnostna *kultura* (Kury et al., 2009; Lobnikar et al., 2012) in primerna *organizacijska dinamika* (Čaleta et al., 2011).

Specifična študija za Slovenijo je v tem oziru novost, saj gre za poglobitev analize 309 vprašalnikov iz pretežno velikih podjetij in relativno izobraženih respondentov. Potrdila je hipotezo, da respondenti kot uporabniki mobilnih naprav *ignorirajo obstoj kibernetskih groženj*, se ne zavedajo *pomembnosti podatkov* na mobilni napravi in jih *ni strah* pred njihovo izgubo. Iz rezultatov je razvidno, da je pri vsaki spremenljivki prevladujoč delež tistih, ki v grožnje verjame. To pomeni, da se respondenti zavedajo groženj, ki jim pretijo ob rabi mobilnih naprav.

S klaster analizo, metodo razvrščanja v skupine in Ward metodo, potrjeno z metodo diskriminantne analize in testom enakosti skupin, smo razdelili respondente na tri skupine: skupino, ki verjame v grožnje, skupino neodločenih in skupino, ki ne verjame v resnost groženj. Spremenljivke, ki najbolj ločujejo posamezne skupine, smo dobili z diskriminantno analizo s hierarhično metodo (STEPVISE). Ta je pokazala prevzem nadzora nad mobilno napravo in prestrezanje prenosa podatkov kot grožnji, ki imata največji vpliv znotraj skupine, ki v grožnje verjame, ter največji vpliv med vsemi tremi skupinami. To smo potrdili še z Wilksovo lambdo.

Znotraj skupine, ki (najbolj) verjame v grožnje, smo preverili, ali morda uporablja vsebine na mobilni napravi, ki so manj občutljive narave. Morda presenetljivo, a respondenti iz skupine, ki sicer verjamejo v grožnje, imajo na mobilni napravi vsebine, ki bi ob uresničitvi grožnje lahko naredile veliko škode, saj tam hranijo sezname stikov, fotografije, službene in tajne dokumente.

Na koncu smo posebej za skupino, ki verjame v uresničitev groženj, preverili, kako zaščitno ukrepajo. Ugotovili smo, da manj kriptirajo podatke na mobilni napravi, da uporabljajo SMS obveščanje in le dobra polovica uporablja protivirusno zaščito. Več uporabljajo gesla ali PIN za dostop do mobilne naprave in podatke sinhronizirajo z drugimi napravi, pri čemer se izognejo izgubi podatkov, nikakor pa ne odtekanju podatkov nepooblaščenim osebam.

Sklepno ugotavljamo, da znanje oziroma vednost o grožnjah ni dovolj. To potrjuje psihološke uvide, da znanje samo po sebi še ne sproži sprememb v obnašanju, premiki so odvisni od motivacije in namenov ljudi (Lobnikar et al., 2012: 351, 359). Znanje ne zadošča, odnos posameznika je ključen. Z drugimi besedami, vednost o tem ne pomaga, če je ne spremlja tudi motiviranost posameznika, za katero bodo morale poskrbeti tudi organizacije. Vpeljava mobilnih naprav v organizacijo in hkrati zagotavljanje kibernetske varnosti mora biti celovit proces. Organizacije morajo sprejeti in uveljaviti pravilnike in standarde, s katerimi bodo definirale celovit način rabe mobilnih naprav med njihovimi zaposlenimi. Na ta način bo jasno določeno, katere vsebine posameznik lahko uporablja in shranjuje na mobilni napravi in katere varnostne rešitve mora uporabljati. Z uvedbo ciljnih izobraževanj bodo organizacije svoje zaposlene izobrazile in ozavestile o načinih varne rabe mobilnih naprav, hkrati pa poskrbele za motivacijo in skupinsko dinamiko. Šele sistemski pristop k problematiki, ki vsebuje vpeljavo standardov rabe mobilnih naprav in tudi izobraževanja o njihovi varni rabi, je lahko uspešen.

Literatura

1. Belgian Cyber Security Guide. (2014). *ISACA & ICC Belgium & VBO-FEB & EY Belgium & Microsoft Belgium & BCCENTRE.* Pridobljeno na http://www.iccbelgium.be/BCSG-EN.pdf
2. Bernik, I. (2014). *Cybercrime and cyberwarfare*. London: ISTE; Hoboken: Wiley.
3. Bernik, I. in Markelj, B. (2014). Zagotavljanje varnosti informacij z razumevanjem uporabnikovega ravnanja z mobilno napravo. *Varstvoslovje, 16*(1), 5–15.

4. 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.
5. Bernik, I. in Prislan, K. (2012). Upravljanje varnostnih tveganj pri rabi mobilnih naprav. V I. Bernik in G. Meško (ur.), *Zbornik prispevkov konference Informacijska varnost: odgovori na sodobne izzive,* (str. 4–5). Ljubljana: Fakulteta za varnostne vede Univerze v Mariboru.
6. Brodkin, J. (2008). *Gartner: Seven cloud computing security risks*. Pridobljeno na http://www.networkworld.com/article/2281535/data-center/gartner--seven-cloud-computing-security-risks.html
7. CES 2016. (2016). 10 of the best gadgets at CES 2016. *The star*. Pridobljeno na http://www.thestar.com/business/2016/01/05/10-of-the-best-gadgets-at-ces-2016.html
8. Chicone, R. G. (2009). *An exploration of security implementations for mobile wireless software applications within organizations* (Doktorska disertacija). Minneapolis: Graduate Faculty of the School of Business and Technology Management.
9. Čaleta, D., Rančigaj, K. in Lobnikar, B. (2011). The nature of security culture in a military organization: a case study of the Slovenian Armed Forces. *Varstvoslovje, 13*(2), 222–239.
10. Čaleta, K. in Čaleta, D. (2012). Vpliv kadrovskega menedžmenta na krepitev varnostne kulture v korporativnovarnostnem okolju. *Sodobni vojaški izzivi 14*(4), 101–122.
11. Delovna skupina iz člena 29. (2014). *Opinion 8/2014 on the recent developments on the internet of things*. Pridobljeno na http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf
12. Direktiva 2002/21/ES Evropskega parlamenta in Sveta z dne 7. marca 2002 o skupnem regulativnem okviru za elektronska komunikacijska omrežja in storitve. (2002). *Uradni list EU*, (L 108).
13. Direktiva 2013/40/EU Evropskega parlamenta in Sveta z dne 12. avgusta 2013 o napadih na informacijske sisteme in nadomestitvi Okvirnega sklepa Sveta 2005/222/PNZ. (2013). *Uradni list EU*, (L 218).
14. Doria, A. (2007). What do the words »internet security« mean? V W. Kleinwächter (ur.), *The power of ideas: Internet governance in a global multi-stakeholder environment* (str. 197–207)**.** Berlin: Druckerei J. Humburg GmbH.
15. Evropska komisija. (2013a). *Skupno sporočilo Evropskemu parlamentu, Svetu, Evropskemu Ekonomsko-socialnemu odboru in Odboru regij: Strategija kibernetske varnosti Evropske unije: odprt, varen in zavarovan kibernetski prostor*. Pridobljeno na http://www.europarl.europa.eu/meetdocs/2014_2019/documents/join/com_join(2013)0001_/com_join(2013)0001_sl.pdf
16. Evropska komisija. (2013b). *Predlog Direktive Evropskega parlamenta in Sveta z dne 7.2.2013 o ukrepih za zagotavljanje visoke skupne ravni varnosti omrežij in informacij v Uniji*. Pridobljeno na http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2013)0048_/com_com(2013)0048_sl.pdf
17. Evropska komisija. (2014). *Poročilo Komisije: Primerjalna analiza uvedbe pametnega merjenja v EU-27 s poudarkom na električni* energiji (COM(2014) 356 final). Pridobljeno na http://ec.europa.eu/transparency/regdoc/rep/1/2014/SL/1-2014-356-SL-F1-1.Pdf
18. Evropska komisija. (2015). *Network and information security directive: co-legislators agree on the first EU-wide legislation on cybersecurity*. Pridobljeno na https://ec.europa.eu/digital-agenda/en/news/network-and-information-security-directive-co-legislators-agree-first-eu-wide-legislation
19. Feldman, J. (30. 4. 2012). Research: 2012 IT spending priorities survey. *Information Week*. Pridobljeno na http://reports.informationweek.com/abstract/83/8816/it-business-strategy/research-2012-it-spending-priorities-survey.html
20. Gostič, Š. (2008). Osnovni principi organizacije korporativne varnosti. V J. Šifrer (ur.). *Javna in zasebna varnost: zbornik prispevkov / 9. slovenski dnevi varstvoslovja* (str. 8). Ljubljana: Fakulteta za varnostne vede. Pridobljeno na http://www.fvv.um.si/dv2008/zbornik/clanki/Gostic.pdf
21. Harcourt, B. E. (2015). *Exposed. Desire and disobedience in the digital age*. Harvard: University Press.
22. Herath, T. in Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154–165.
23. Inštitut Jožef Štefan [IJS]. (2016). *Kako izbrati dobro geslo (in si ga zapomniti)*. Pridobljeno na https://www.ijs.si/ijsw/Kako%20izbrati%20dobro%20geslo%20%28in%20si%20ga%20zapomniti%29
24. Juniper Networks. (2010). *Mobile security – why the time is now.* Pridobljeno na http://www.techrepublic.com/resource-library/whitepapers/mobile-security-why-the-time-is-now/
25. Juniper Networks. (2011a). *Malicious mobile threats report 2010/2011*. Pridobljeno na http://www.juniper.net/us/en/dm/interop/go
26. Juniper Networks. (2011b). *Mobile device security – emerging threats, essential strategies*. Pridobljeno na http://www.adtech-global.com/Data/Sites/1/marketing/juniperwhitepapermobiledevicesecurity.pdf
27. Kanduč, Z. (2015). Neoliberalna globalizacija, razredni nadzor, kriminalno vprašanje in politični odgovori. V A. Šelih in K. Filipčič (ur.), *Kriminologija* (str. 632–674). Ljubljana: IUS Software, GV založba: Inštitut za kriminologijo pri Pravni fakulteti.
28. Kanellos, M. (13. 1. 2016). Hold the laughter: Why the smart fridge is a great idea. *Forbes.* Pridobljeno na http://www.forbes.com/sites/michaelkanellos/2016/01/13/hold-the-laughter-why-the-smart-fridge-is-a-great-idea/#6c25e74256f5
29. Kaspersky Lab. (2015a). *Personal devices and corporate secrets: Only 11% of people worry about keeping work files safe on mobile devices, kaspersky lab survey shows.* Pridobljeno na http://www.kaspersky.com/about/news/product/2015/Personal-Devices-and-Corporate-Secrets-Only-11-of-People-Worry-about-Keeping-Work-Files-Safe-on-Mobile-Devices-Kaspersky-Lab-Survey-Shows
30. Kaspersky Lab. (2015b). *Hidden danger: Small businesses dismiss mobile risks, overlooking BYOD threats*. Pridobljeno na http://www.kaspersky.com/about/news/virus/2015/Hidden-Danger-Small-Businesses-Dismiss-Mobile-Risks-Overlooking-BYOD-Threats
31. Kovacs, E. (4. 11. 2015). Contactless Visa cards vulnerable to fraudulent foreign currency transactions. *SecurityWeek.* Pridobljeno na http://www.securityweek.com/contactless-visa-cards-vulnerable-fraudulent-foreign-currency-transactions
32. Kovačič, M. (2012). *Gesla in varna hramba gesel (mala šola informacijske varnosti, 1. del).* Provokator. Pridobljeno na https://pravokator.si/index.php/2012/07/30/gesla-in-varna-hramba-gesel-mala-sola-informacijske-varnosti-1-del/
33. Kury, H., Meško, G., Mitar, M. in Fields, C. (2009). Slovenian police officers attitudes towards contemporary sucurity threats and punishment. *Policing: An International Jounrmal of Police Strategies & Management, 32*(3), 415–429.
34. Lobnikar, B., Prislan, K., Markelj, B. in Banutai, E. (2012). Informacijsko-varnostna ozaveščenost v javnem in zasebnem sektorju v Sloveniji. *Varstvoslovje, 14*(3), 345–363.
35. Lookout. (2011). *Lookout mobile threat report*. Pridobljeno na https://www.lookout.com/static/ee_images/lookout-mobile-threat-report-2011.pdf

36. Markelj, B. (2014). *Grožnje informacijski varnosti pri rabi mobilnih naprav* (Doktorska disertacija). Ljubljana: Fakulteta za varnostne vede Univerze v Mariboru.
37. McAfee, A. (1. 8. 2011). The rise of the virtual office. *Technology review.* Pridobljeno na http://www.technologyreview.com/news/424871/the-rise-of-the-virtual-office/
38. McAfee. (2012). *McAfee threats report: first quarter 2012*. Pridobljeno na http://www.McAfee.com/us/resources/reports/rp-quarterly-threat-q1-2012.pdf
39. Newcomb, D. (22. 2. 2013). FCC ruling could set connected cars and Wi-Fi on collision course. *Wired*. Pridobljeno na http://www.wired.com/2013/02/fcc-wifi-connected-cars/
40. Norton, K. (24. 10. 2012). *Mobile security: 6 reasons devices remain vulnerable*. Pridobljeno na http://deloitte.wsj.com/cio/2012/10/24/mobile-security-6-reasons-devices-remain-vulnerable/
41. Olavsrud, T. (9. 1. 2013). Mobile attacks top the list of 2013 security threats. *CIO.* Pridobljeno na http://www.cio.com/article/2389296/security0/mobile-attacks-top-the-list-of-2013-security-threats.html
42. Open Web Application Security Project [OWASP]. (2013). *OWASP mobile security project*. Pridobljeno na https://www.owasp.org/index.php/OWASP_Mobile_Security_Project
43. Organizacija za ekonomsko sodelovanje in razvoj [OECD]. (2002). *Guidelines for the security of information systems and networks.* Pridobljeno na http://www. oecd.org/dataoecd/16/22/15582260.pdf
44. Pešić, M. (2015). *Varnost v mobilnih sistemih Android in iOS, programska oprema za forenziko in primera mobilne forenzike na obeh platformah* (Diplomsko delo). Ljubljana: Fakulteta za varnostne vede Univerze v Mariboru.
45. *Safe.si*. (2016). Varna gesla. Pridobljeno na: http://safe.si/podrocja/moja-identiteta-in-zasebnost-na-spletu/varna-gesla
46. Skupni raziskovalni center Evropske komisije. (2014). *Over 70% European consumers to have a smart meter for electricity by 2020*. Pridobljeno na https://ec.europa.eu/jrc/en/news/over-70-percent-european-consumers-have-smart-meter-electricity-2020
47. Statistični urad Republike Slovenije [SURS]. (2014). *Podjetja po pravnoorganizacijski obliki in velikosti glede na število oseb, ki delajo (SKD 2008), Slovenija, letno*. Pridobljeno na http://pxweb.stat.si/pxweb/Dialog/varval.asp?ma=2430104S&ti=&path=../Database/Ekonomsko/24_zunanja_trgovina/02_24301_blagovna_menjava/&lang=2
48. Statistični urad Republike Slovenije [SURS]. (2015). *Elektronske komunikacijske storitve, Slovenija, 4. četrtletje 2014*. Pridobljeno na http://www.stat.si/StatWeb/prikazi-novico?id=5083&idp=25&headerbar=16
49. Statistični urad Republike Slovenije [SURS]. (2016). *Dan varne uporabe interneta 2016.* Pridobljeno na http://www.stat.si/StatWeb/prikazi-novico?id=5747&idp=25&headerbar=16
50. Varni na internetu. (2013). *ABC varnosti in zasebnosti na mobilnih napravah*. Pridobljeno na https://www.varninainternetu.si/content/uploads/2013/01/Varnost-in-zasebnost-na-mobilnih-napravah.pdf
51. WEB-Center. (2012). *Pregled groženj v letu 2012*. Pridobljeno na http://www.web-center.si/pregled-grozenj-v-letu-2012/
52. Zakon o obrambi. (2004). *Uradni list RS,* (103/04, 95/15).
53. Završnik, A. (2015). *Kibernetska kriminaliteta*. Ljubljana: IUS Software, GV založba: Inštitut za kriminologijo pri Pravni fakulteti.
54. Završnik, A. in Levičnik, P. (2014). Zasebnost po Snowdnu: novejša teoretična razumevanja zasebnosti in odnos javnosti do nje v Sloveniji. *Zbornik znanstvenih razprav, 74*, 117–152.

Revija za kriminalistiko in kriminologijo / Ljubljana 67 / 2016 / 1, 44–60

The Corporate Cyber Security of Mobile Devices: The Awareness of Slovenian Users

Blaž Markelj, Ph.D., Lecturer of Information Science at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. E-mail: blaz.markelj@fvv.uni-mb.si

Aleš Završnik, Ph.D., Senior Research Fellow at the Institute of Criminology at the Faculty of Law, University of Ljubljana, and Associate Professor at the Faculty of Law, University of Ljubljana, Slovenia. E-mail: ales.zavrsnik@pf.uni-lj.si.

Mobile devices have become the central node information-communication technology as they include functionalities far surpassing simply making a phone call. Along with the merging of services and functionalities on a single mobile device, the importance of users' perceptions and understanding of cyber security threats has grown substantially. A lack of knowledge of the principles of safe usage of mobile devices also increases the risk for systems and data of organisations either accessed with users' mobile devices or stored on their devices.

Fundamental notions and terminology, such as cyber or information security, network and information security (NIS), and cybercrime are defined in the first part of the paper. Furthermore, it presents the new trends in NIS legislation at the European Union level and shows the most recent statistical trends, which reflect the high level of mobile device penetration in the corporate world. In the second part of the paper, research conducted among Slovenian organisations on users' knowledge of cyber security threats, the level of risk taken while using mobile devices for business purposes, and the cyber security protective measures employed, is presented.

Keywords: cyber security, mobile devices, corporate security, cybercrime, network and information security (NIS)

UDC: 004.056