Kombinirane grožnje rabe mobilnih naprav v poslovne namene

Blaž Markelj, Fakulteta za varnostne vede, Univerza v Mariboru
Igor Bernik, Fakulteta za varnostne vede, Univerza v Mariboru

Namen
Nepoznavanje uporabe mobilnih naprav lahko resno ogrozi informacijski sistem celotne organizacije. Šibki točki informacijskega sistema sta tako uporabnik, kot tehnologija - mobilne naprave (prenosniki, pametni telefoni, dlančniki,..), ki omogočajo lažjo komunikacijo in hitrejši dostop do podatkov. Poznavanje pravilne uporabe (z varnostnega vidika) izročenih sredstev je pomembno, zato je izobraževanje uporabnikov in organizacij nujno.

Metodologija
S pomočjo deskriptivne metode je narejen pregled literature. Ker je primarna literatura skopa, bodo analizirani tudi sekundarni viri. Predstavljeni bodo tudi podatki rabe podjetij in analizirane grožnje, ki prežijo na podjetja pri omenjeni rabi.

Ugotovitve
Zaradi nezadosti varne uporabe mobilnih naprav v organizacijah, sklepamo, da so organizacije šele v začetnih fazah zavedanja informacijske nevarnosti ob nenadzorovani uporabi mobilnih naprav. Prispevek predstavlja nekaj smernic za ureditev omenjenega področja.

Omejitve
Prispevek obravnava analizo pregleda obstoječe literature na temo kombiniranih groženj informacijski varnosti posameznih organizacij – nevarnost se pojavi pri uporabi mobilnih naprave. Zaradi novosti teme se pojavijo omejitve že pri obstoječi literaturi in predhodnih raziskavah, ki so zelo skope.

Praktična uporabnost
Predstavljen bo model, ki bo organizacijam lahko v pomoč pri ocenitvi trenutnega stanja informacijske varnosti in zaščite pred kombiniranimi grožnjami, ko bodo njihovi uporabniki uporabljali mobilne naprave.

Izvirnost
Prispevek predstavlja temo, ki se je veliko organizacij še ne zaveda, večina uporabnikov pa sploh še ne pozna. Kot že omenjeno, so viri na to temo zelo skopi, medtem ko se organizacije šele začenjajo zavedati pomena izpostavljenosti nevarnosti izgube informacij in posledično nezaupanja v njihovo poslovanje.

Ključne besede: informacijska varnost, kombinirane grožnje, mobilne naprave, poslovanje

1 Uvod

Hiter način življenja, pospešeni poslovni procesi ter vsakodnevno sprejemanje pomembnih odločitev, tako poslovnih kot zasebnih, so ustvarili potrebo po hitrem, zanesljivem in stalnem dostopu do informacij. Z bliskovitim razvojem tehnologije in spremenjenimi načini komuniciranja si je skoraj nemogoče zamišljati, da človek ne bi imel zagotovljenega praktično stalnega dostopa do podatkov in informacij. Mobilne naprave, katerih število se iz leta v leto močno povečuje, v zadnjih mesecih pa doživljamo pravi bum, nam omogočajo enostavno povezovanje v svet informacij. V zadnjih letih ni napredoval samo razvoj mobilnih naprav, temveč se je zgodilo marsikaj tudi v razvoju spletnih povezav (tudi brezžičnih) in pri centralizaciji informacijskega okolja organizacij. Tako ima uporabnik v vsakem trenutku neomejen dostop do poslovnih informacij in osnovo za lažje, hitrejše delo in odločanje. Poznavanje učinkovite in varne uporabe mobilnih naprav lahko razumemo tudi kot konkurenčno prednost v tekmi za prevlado v gospodarskem in znanstvenem svetu. S tem pa se na drugi strani odpirajo varnostna vprašanja glede dostopa v sistem. Z zmanjševanjem možnosti za nepooblaščen in/ali zlonameren vdor v informacijski sistem, odtujitev in zlorabo informacij se krepi zaupanje v procese, transakcije in informacije, s katerimi se operira v določenem okolju, zato je vzpostavljanje in vzdrževanje varnega dostopa do informacijskega sistema organizacije nujno (Saksida, 2008).

Praktično vsak mobilni telefon omogoča povezavo s svetovnim spletom, vstop v informacijski sistem organizacije in upravljanje z podatki. Posamezne organizacije zaradi lažjega dostopa do informacijskega delovnega okolja celo namerno puščajo »odprta vrata«. S tem omogočijo enostavnejše zlorabe in vstop v informacijski sistem organizacije tudi drugim uporabnikom spleta. Z varnostnega vidika so poleg poznanih in enostavnih groženj (razni napadi, odtujitve, ...) nevarne zlasti kombinacije raznovrstne programske opreme, ki se nahaja na mobilnih napravah, dostopa prek javnih omrežij, nezaščiteni certifikati in možnost odtujitve naprave. Določeni programi namreč omogočajo avtomatičen cikličen prenos podatkov iz informacijskega sistema organizacije na uporabnikov telefon, ko ta vpiše vanj svoje podatke: uporabniško ime, geslo in določene podatke strežniškega sistema. Vprašanje je, koliko je mogoče zaupati programski opremi, ki deluje avtomatično. Kaj program, ki samodejno deluje, v ozadju pravzaprav počne? Kaj se zgodi, če nam telefon ukradejo? V telefonskem aparatu so poleg ostalih pomembnih, ne nazadnje shranjeni tudi podatki za prijavo v domeno in strežniški sistem (Chickowski, 2009). Tako je v primeru vdora v telefon, prisluškovanja povezovanju prek javnih omrežij ali odtujitve aparata vsebina podatkov enostavno na voljo napadalcem!

S pričetkom uporabe mobilnih brezžičnih komunikacijskih naprav smo podrli mejo med komunikacijo znotraj informacijskega sistema organizacije in zunanjim svetom. Danes je svet prepreden s komunikacijsko mrežo: vsak lahko komunicira z vsakomur, nalaga in prenaša podatke. Dostopi do pomembnih podatkov so zelo enostavni in žal, z vidika informacijske varnosti, veliko premalo zaščiteni. Strokovnjaki za razvoj varnostne strojne in programske informacijske tehnologije iščejo optimalne načine analiziranja in nadzorovanja vsebine, ki se pretaka po komunikacijskih kanalih. Smernice razvoja kažejo, da bo tehnologija v prihodnosti omogočala analizo spletnega prometa in celotnega informacijskega sistema na podlagi zaznanih sprememb (odstopanja od rutine). Danes pa žal še nimamo enostavnih, predvsem pa za uporabnike transparentnih rešitev, ki bi zaščitile informacijske sisteme organizacij pred zlorabami.

Organizacije tveganja zmanjšujejo tako, da implementirajo strojno opremo, ki pregleduje potencialne nevarnosti na ravni spletnega prometa (Whitman, Matorord, 2008), in posebne naprave, ki preprečujejo vdore v informacijski sistem (Scarfone, Mell, 2007). Nekatera podjetja, ki razvijajo varnostno programsko opremo, uporabnikom že nudijo tudi napredne

varnostne programe za mobilne naprave (Schechtman, 2011) in programske požarne zidove, ki pregledujejo spletni promet tako na mobilnih napravah kot v informacijskem sistemu organizacije (Endait, 2011). Ustrezna programska oprema omogoča tudi, da organizacije same določijo notranja pravila varne uporabe mobilnih naprav (Mottishaw, 2010). V večini organizacij mora imeti uporabnik (uslužbenec) zaradi varnosti geslo za vstop v brezžična omrežja (Arbaugh, 2010). Nekatere organizacije so uveljavile interne pravilnike za zagotavljanje informacijske varnosti, ko so urejale dokumentacijo za pridobitev certifikata ISO 27001 (Calder, 2006, Bernik, Prislan, 2011).

2 Varna raba mobilnih naprav

Uporabnikov mobilnih naprav je, kot že ugotovljeno vsako leto več. Najbolj so razširjene preproste mobilne naprave, ki so se razvile iz mobilnih telefonov in uporabniku poleg telefoniranja zagotavljajo hiter dostop do potrebnih informacij. Če rečemo, da je bil razvoj prenosne informacijske tehnologije hiter in učinkovit, pa moramo hkrati žal ugotoviti, da je bilo zelo malo narejenega glede varnosti dostopa do informacij in prenosa le-teh. Če uporabnik deluje znotraj informacijskega okolja organizacije, z definiranimi varnostnimi standardi, je mogoče dokaj učinkovito poskrbeti za informacijsko varnost. Varnost se zagotavlja v okviru standardiziranega varovanja celotnega informacijskega okolja organizacije in to s postopki, ki so se razvili v zadnjih petdesetih letih.
Nevarnost vdora v informacijski sistem in zlorabe podatkov je veliko večja, kadar je uporabnik zunaj varovanega informacijskega okolja organizacije, to je v javno dostopnem omrežju, od koder se lahko poveže s omrežjem organizacije in s pomočjo preprostih, nevarovanih protokolov oz. programov. Poznamo več načinov povezovanja, ki jih uporabljajo mobilne naprave ob prenosu podatkov iz okolja organizacije. Uporabnik se mora zavedati, da se prav ob vsaki vzpostavitvi zveze, naredi »tunel« skozi zunanjo zaščito omrežja organizacije, s tem pa se pojavi informacijsko tveganje za celotno organizacijsko infrastrukturo. Podatki in informacije, ki jih prenašamo (npr. elektronska pošta, dokumenti ali prijave v določene aplikacije znotraj informacijskega sistema organizacije – prenos podatkov med aplikacijami strežnika in odjemalca) so tako relativno lahko dostopni tistim, ki bi jih želeli pridobiti, pri tem pa ne potrebujejo niti specialnega znanja in priprav, saj je dostop in prenos podatkov slabo zaščiten. Ko gre za vdore v sistem, sta trenutno najšibkejša člena uporabnik in njegova mobilna naprava, s katero skozi »posebna vrata« vstopa v sistem organizacije. Zelo pomembno je, da uporabnik mobilne naprave dobro pozna standarde varne uporabe. Pravzaprav morajo organizacije poskrbeti za izobraževanje in kakovostno oblikovane pravilnike, ki določajo standarde uporabe, predvideti ukrepe, ki sledijo nepravilni ali zlonamerni uporabi mobilnih naprav. Standardi naj določajo dovoljeno uporabo programske in strojene opreme ter protokole za varno povezovanje v omrežja in korporativni informacijski sistem (Allen, 2006; Whitman, Matorord, 2008).

3 Programska oprema mobilnih naprav

Učinkovitost mobilnih naprav je v veliki meri odvisna od nameščene programske opreme in tega, kako se povezuje in prilagaja delovanju večjih sistemov. Razvoj programske opreme za mobilne naprave je večinoma sledil splošnemu trendu razvoja informacijske tehnologije. Velik poudarek je bil dan predvsem enostavnejšim programom, ki na mobilni napravi delujejo kot pripomočki, da uporabnik enostavneje in hitreje pride do želenih podatkov in/ali informacij. Ti

pripomočki predstavljajo nov način komunikacije ali le omogočajo hitrejšo izvedbo opravila. Varnost takšne programske opreme je vprašljiva, saj uporabnik pogosto ne pozna njenega izvora in ne ve natanko, kako programi, ki si jih je naložil na mobilno napravo dejansko delujejo. Programska oprema, ki se na prvi pogled ne zdi nevarna, lahko brez vednosti uporabnika »deluje v ozadju« mobilne naprave in omogoča zlonamerna dejanja. Za uporabo določene programske opreme (npr. za sinhronizacijo elektronske pošte) mora uporabnik vpisati svoje podatke (se prijaviti v domensko okolje organizacije). Zato je potrebno programsko opremo na mobilni napravi razumeti kot celoto. Za kršenje načel informacijske varnosti oz. za odtujitev podatkov in informacij je treba namestiti na mobilno napravo samo delček nevarne programske opreme. Zato je potrebno programsko opremo mobilne naprave iz varnostnega vidika preveriti in se prepričati, da ji uporabnik lahko zaupa. Tudi predhodno nameščeno programsko opremo na mobilnih telefonih je potrebno preveriti in zagotoviti, da deluje kot je predvideno. Posamezne funkcije in programsko opremo naprave, ki dostopa do omrežja na kakršen koli način, je smiselno izključiti za čas ko jih ne potrebujemo, saj s tem zmanjšamo možnost vdora v našo mobilno napravo. V nasprotnem primeru preko vklopljene programske opreme in povezovalnih funkcij lahko v mobilno napravo vdrejo. Kot primer lahko navedemo vdor preko vklopljene »bluetooth« povezave (Shilton, 2009). Smiselno bi bilo, da bi ustvarjalci in ponudniki, tako mobilnih naprav kot programske opreme določili standarde in na podlagi teh tudi certificirali svoje izdelke. Hkrati bi morala vsaka organizacija sama določiti notranje standarde uporabe programske opreme na mobilnih napravah, ki bi seveda nastali na podlagi certifikatov strojne in programske opreme.

4 Sredstva in pravilnik varne uporabe mobilnih naprav

Poznavanje pravilne in varne rabe mobilnih naprav in programskih dodatkov zanje lahko razumemo kot konkurenčno prednost v tekmi za prevlado v gospodarskem in znanstvenem svetu. Informacijska varnost je ključni element integritete vsake organizacije, njenih zaposlenih, poslovnih procesov in informacij, s katerimi operira. Pomanjkljivo znanje zaposlenih o varni rabi mobilnih naprav in pomanjkanje internih varnostnih standardov lahko pripeljejo organizacijo v težaven položaj. Prva šibka točka vsakega informacijskega sistema je nepoučen uporabnik, druga pa pomanjkanje standardov, ki bi opredeljevali varno uporabo strojne in programske opreme. Zaradi hitrega razvoja informacijske tehnologije in zato, ker to danes uporablja večino zaposlenih, je nujno potrebno poskrbeti za neprestano izobraževanje in informiranje uporabnikov o nevarnostih in pasteh sodobne tehnologije. Cilj organizacije bi moral biti, da se vsa izročena sredstva (to so: programska in strojna oprema ter pravilniki, ki določajo standarde informacijske varnosti) uporabljajo varno.
Raba mobilnih naprav je varna takrat, kadar se mobilne naprave uporabljajo v skladu s sprejetimi varnostnimi pravili, ki jih organizacije sprejmejo na podlagi naslednjih izhodišč:

- Organizacija si zagotovi boljšo varnost svojega informacijskega sistema tako, da uporabo izročenih sredstev določi z lastnimi standardi in internimi pravilniki.
- Pravilniki so dejavnik nadzora in delujejo kot preventiva za primere neodgovorne in tvegane uporabe mobilnih naprav v okviru poslovanja organizacije.
- S pravilnikom organizacija določi, kako in na kakšen način ter s kakšnim namenom se uporabljajo mobilne naprave in programska oprema na njih. S tem organizacija poskrbi za bolj varne poslovne procese.
- Interni pravilniki določajo tudi krivdno odgovornost uporabnika (zaposlenega) ali organizacije, če pride do škode zaradi malomarne uporabe mobilnih naprav.

Če organizacija uspe, s pomočjo izobraževanja in pod pritiskom sprejetih pravil, zagotoviti, da uporabniki bolj vestno ravnajo z opremo in so pazljivi pri vstopanju v informacijsko okolje organizacije, ji bo uspelo precej zmanjšati vpliv kombiniranih groženj.

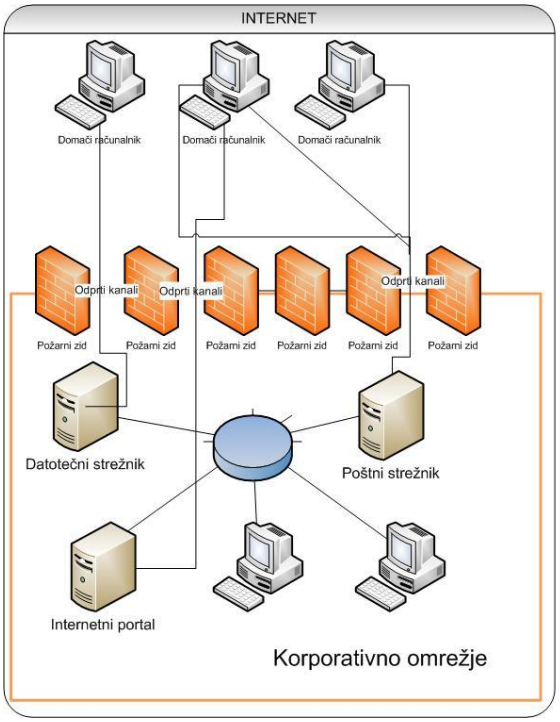
5 Kombinirane grožnje

Mobilne naprave so tarče različnih groženj, z namenom, da se nepooblaščeno pridobi občutljive informacije in se z njimi okoristi. Ker se grožnje lahko ponavljajo na različnih segmentih in ker lahko več različnih groženj deluje simultano oziroma v kombinaciji, jih imenujemo kombinirane grožnje. Take grožnje predstavljajo veliko nevarnost organizacijam in posameznikom (Markelj, Bernik, 2011). Ko se uporabnik z mobilno napravo poveže s spletom in s pomočjo tega z informacijskim okoljem organizacije, se v trenutku izpostavi različnim grožnjam. Nevarnosti so lahko neposredne ali posredne; torej se različne grožnje med seboj kombinirajo. Ena najbolj neposrednih groženj je odtujitev mobilne naprave uporabniku. Če ima na njej shranjene pomembne dokumente in informacije o informacijskem sistemu organizacije, vključno s podatki za dostop in verifikacijo, nima pa omogočene niti najosnovnejše zaščite (kot je npr. PIN) je krivda pri eventualni zlorabi na strani uporabnika. Bolj sofisticirani grožnji sta prestrezanje komunikacije, ko se uporabnik poveže v svetovni splet z javno dostopne točke in dostopa do informacijskega sistema organizacije in podtikanje programske opreme, ki samodejno poskrbi za odtujitev informacij. Posredne grožnje so največkrat hujše, saj so nepredvidljive – pred njimi pa se ni mogoče stoodstotno zavarovati.

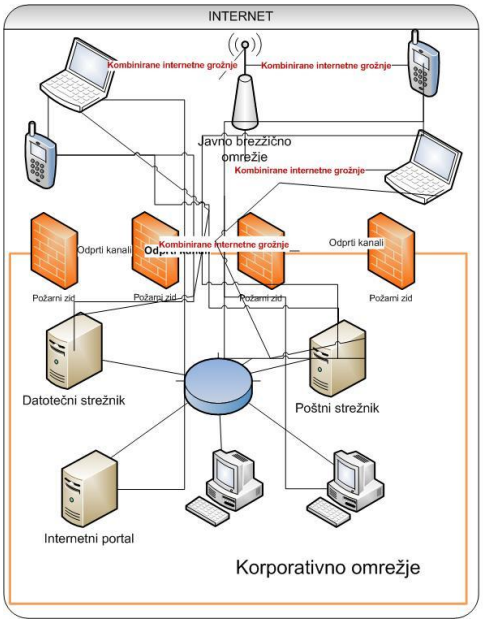
Sodobne komunikacije, dostopi v informacijsko omrežje organizacije in načini povezovanja so precej drugačni, kot še do nedavnega. Slika 1 nazorno prikazuje razliko v komunikaciji med centralnim omrežjem – intranetom – in svetovnim spletom, ter razlike v potencialni ogroženosti.

V preteklosti je zadoščalo, če je bilo informacijsko omrežje organizacije varovano s požarnim zidom, saj komunikacija iz zunanjega omrežja ni prehajala v notranje omrežje brez dovoljenja požarnega zidu. Hkrati ni bilo naprav, ki bi bile zunaj centralnega omrežja, se povezovale v informacijsko omrežje organizacije in hkrati komunicirale z zunanjim svetom s pomočjo drugih sistemov, npr. WiFi, UMTS idr. Danes uporabnik izbira med številnimi mobilnimi napravami, iz njimi istočasno, kljub požarnemu zidu, komunicira prek različnih omrežij. Požarni zid dovoli komunikacijo med mobilno napravo in centralnim sistemom, vendar mobilna naprava, ki se uporablja zunaj centralnega omrežja in komunicira tudi z zunanjim svetom (javno dostopnim omrežjem), predstavlja šibko točko celotnega informacijskega sistema organizacije. S »posegom« v mobilno napravo, do katerega pride, ker je ta povezana s spletom (slika 2), se odpre nenadzorovana pot od mobilne naprave do centralnega sistema, saj je požarni zid komunikacijo mobilni napravi že dovolil.

Ker mobilna naprava komunicira z več omrežji hkrati, dostop v informacijsko omrežje skozi varnostne sisteme pa je že vzpostavljen, je uporabnik v položaju, ko njegovo mobilno napravo ogrožajo kombinirane grožnje. Preko mobilne naprave je tako ogroženo premoženje podjetja (podatki in informacije) znotraj informacijskega omrežja organizacije. Grožnje, ki so nekdaj prežale na uporabnika na komunikacijski poti (in ki se jim je naučil izogniti s poznanimi ukrepi in napravami), danes zaradi kombinacije učinkov postajajo resen problem za varnost organizacije. Rešitve, ki bodo zagotovile višjo stopnjo varnosti in zmanjšale vplive omenjenih groženj, so sicer v razvoju, žal pa zaradi pomanjkanja standardov le-te vsaj dolgoročno ne bodo ves čas optimalno učinkovite – potrebno bo stalno spremljanje položaja in prilagajanje sistemov v razvoju.



Slika 1: Komunikacija informacijskega sistema organizacije s spletom skozi požarni zid (v preteklosti).



Slika 2: Komunikacija informacijskega sistema organizacije z mobilnimi napravami in komunikacija mobilnih naprav s spletom

Od posameznika in organizacije je odvisno, kako in na kakšen način poskrbijo za varno dostopanje v informacijske sisteme in kako varujejo zasebne in/ali delodajalčeve poslovne podatke. V preteklosti je bilo čutiti veliko potrebo po zagotavljanju varnosti informacijskega

sistema organizacije, danes pa se – zaradi hitrega razvoja in čedalje pogostejše rabe mobilnih naprav – povečuje tudi potreba po učinkoviti informacijski varnosti le-teh (Boudriga, 2010). Informacijski sistem je ranljiv toliko kot je ranljiv njegov najšibkejši člen. Zaradi tega se je potrebno osredotočiti na dele sistema, ki so manj obvladljivi, to so predvsem mobilne naprave. Naprave je potrebno zaščititi in poskrbeti za ustrezno zaščito pred kombiniranimi grožnjami (International Data Group Company, 2011).
Za varnost mobilnih naprav in podatkov, ki se nahajajo na njih lahko poskrbimo tudi tako, da se zavedamo, da informacijska nevarnost obstaja, in kakšne so lahko posledice (European Network and Information Security Agency - ENISA, 2010). Eden izmed načinov, da se organizacija zaščiti, je, da poskrbi za dobro politiko informacijske varnosti (Bernik, Prislan, 2010). Dobra varnostna politika zajema standardizirana navodila za varno uporabo mobilnih naprav. Iz te pa se izvede interne pravilnike, ki določajo, katera strojna in programska oprema velja za standardno znotraj organizacije (Simt, 2009). Poskrbeti je potrebno še za mrežni nadzor prometa, požarne zidove, enkripcijo podatkov in sledenje ter omogočiti oddaljeno brisanje podatkov z mobilnih naprav v primeru odtujitve. Pri tem pa mora ustrezati standardom in priporočilom za zagotavljanje informacijske varnosti tudi zaščita avtorizacije v informacijskem sistemu (Chickowski, 2009).

6 Zaključek

Razvoj tehnologij za zagotavljanje ustrezne informacijske varnosti gre v smer analize internetnega prometa in obnašanja sistemov. Temelji na načelu ugotavljanja odstopanja od standardnega obnašanja, naj si gre za sistem ali internetni promet. Še vedno pa se v veliki meri pozablja oz. zanemarja človeški faktor, ki upravlja z informacijsko tehnologijo in kot smo že omenili s svojim nepravilnim upravljanjem izročenih sredstev predstavlja najšibkejši člen v informacijski varnosti. Zato je pomembno, da se organizacije zavedo, da se ne morejo izogniti valu vedno naprednejše mobilne informacijske tehnologije. Zato je potrebo spoznati pomembnost izobraževanja zaposlenih in s tem posledično zmanjšat riziko nevarnosti, ki na organizacijo pretijo zaradi rabe mobilnih naprav. Pomembno je tudi da se znotraj organizacij oblikujejo pravilniki, ki s pomočjo standardov določajo za organizacijo varno uporabo izročenih sredstev in na podlagi že obstoječe informacijske tehnologije določajo, katere mobilne naprave in katera programska oprema je za njihovo organizacijo primerna in hkrati dovoljena.
Razvoj modernih mobilnih naprav in njihove programske opreme je zelo hiter in nepredvidljiv. Zato je nujno narediti sistem fleksibilen in varen z vidika informacijske varnosti. Današnje tendence varnostnih sistemov le parcialno pokrivajo mobilne naprave in njihove tehnologije, ni pa sistema, ki bi bil sposoben s stališča varnosti nadzorovati in kontrolirati delovanje, povezovanje in podatkovne prenose mobilnih naprav znotraj posameznih organizacij.

7 Literatura

Allen, M. (2006). Mobile Security. *The Journal of International Security, 16*(6), 25-27.

Arbaugh, W. (2003). *Wireless Security Is Different*. Pridobljeno 5. 3. 2011 na svn.assembla.com/svn/odinIDS/Egio/artigos/.../Firewall/01220591_IMP.pdf.

Bernik, I. in Prislan, K. (2010). Proces upravljanja s tveganji v informacijski varnosti. V P. Umek in T. Pavšič Mravlje (ur.)*, Smernice sodobnega varstvoslovja [Elektronski vir]: zbornik prispevkov*. 11. slovenski dnevi varstvoslovja, Ljubljana, 3.-4. junij 2010. Ljubljana:

Fakulteta za varnostne vede. Pridobljeno 1.3.2011 na http://www.fvv.uni-mb.si/DV2010/zbornik.html.

Bernik, I. in Prislan, K. (2011). Information Security in Risk Management Systems: Slovenian Prospective. V B. Dobovšek in A. Sotlar (ur.), *Varstvoslovje, 13*(2), 208-222.

Boudriga, N. (2010). *Security Of Mobile Communications.* New York: Auerbach Publications.

Calder, A. (2006). Implementing Information Security Based on ISO 27001/ISO 17799: A Management Guide. Hogeweg: Van Haren Publishing B. V.

Chickowski, E. (2009). *10 Mobile Security Best Practices*. Pridobljeno 10. 1. 2011 na http://www.baselinemag.com/c/a/Mobile-and-Wireless/10-Mobile-Security-Best-Practices.

Endait, S. (2010). *Mobile Security – The Time is Now*. Pridobljeno 5. 3. 2011 na http://www.authorstream.com/Presentation/snehaendait-477029-mobile-security.

European Network and Information Security Agency (ENISA). (2010). *The New User`s Guide: How to Rise Informations Security Awareness.* Luxembourg: Publications Office of the European Union.

International Data Group Company. *Security for Mobile Devices on the Corporate Network*. Pridobljeno 15. 1. 2011 na http://www.networkworld.com/newsletters/2010/032210wan1.html.

Markelj, B. in Bernik, I. (2011). Kombinirane grožnje informacijski varnosti pri rabi mobilnih naprav. *Nove razmere in priložnosti v informatiki kot posledica družbenih sprememb [Elektronski vir]: zbornik konference / 18. konferenca Dnevi slovenske informatike,* Portorož, Slovenija, 18.-20. april 2011.

Mottishaw, P. (2010). *Policy Management Will Be Critical to Mobile Operators as Data Traffic Grows*. Pridobljeno 6. 3. 2011 na http://www.analysysmason.com/About-Us/News/Newsletter/Policy-management-has-become-an-urgent-issue-for-mobile-operators-as-a-result-of-the-rapid-growth-in-mobile-data-traffic-increasing-availability-of-flat-rate-data-plans-and-new-regulations-in-Europe.

Saksida, M. (2008). *Preprečite uhajanje podatkov iz omrežja*. Pridobljeno 17. 1. 2011. na http://dne.enaa.com/Racunalniska-oprema/Racunalniska-oprema/Preprecite-uhajanje-podatkov-iz-podjetij.html

Scarfone, K. in Mell, P. (2007). *Guide To Intrusion Detection and Prevention System*. Pridobljeno 4. 3. 2011 na http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

Schechtman, D. (2011). *IPad Security from En Pointe and McAfee's Mobile Security Practice*. Pridobljeno 5. 3. 2011 na http://www.enpointe.com/blog/ipad-security-en-pointe-and-mcafees-mobile-security-practice.

Shilton, K. (2009). Four Billion Litlle Brothers? Privacy, Mobile Phones, and Ubiquitous data Collection. *Communications of the ACM, 52*(11), 48-53.

Simt (2009). *Upravljanje, nadzor in varnost informacijskih sistemov.* Pridobljeno 11. 10. 2011 na http://www.simt.si/informacijski_sistemi.html.

Whitman, M. E. in Matorord, H. J. (2008). *Management of Information and Security, 2nd edition.* Boston: Course Technology Cengage Learning.