Mobilni dostop z vidika informacijske varnosti do podatkov v oblaku

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

Namen
Težnja po hitrem in učinkovitem dostopu do podatkov, ne glede kje se nahajamo, je vedno večja. Zaradi velike rasti uporabe mobilnih naprav in tehnologije, ki nam omogoča da imamo podatke v oblaku, je to popolnoma izvedljivo. Pojavi pa se vprašanje informacijske varnosti. Ali uporabljamo protokole varne povezave v oblak in ali upravljamo z našo mobilno napravo na varen način? Kaj nam pomaga varnost v oblaku, če nepremišljeno (ne-varno) ravnamo z mobilno napravo in omogočimo odtujitev podatkov?

Metodologija
S pomočjo deskriptivne metode je bil narejen pregled literature, zaradi novega področja pa je bila poleg analize primarnih virov narejena tudi analiza sekundarnih virov raziskav v tujini.

Ugotovitve
Zaradi pomakanja virov in raziskav na temo varne uporaben mobilnih naprav in kombiniranih groženj ter skeptičnosti organizacij do prenosa in dostopanja do kritičnih podatkov v oblaku, lahko sklepamo da so organizacije šele z začetnih fazah zavedanja informacijske nevarnosti ob nenadzorovani uporabi mobilnih naprav pri povezavi v oblak.

Omejitve
Zaradi novosti teme se pojavijo omejitve že pri obstoječi literaturi in predhodnih raziskavah, ki so zelo skope, ter seveda pri temi sami, ki je za organizacije zelo občutljivega pomena.

Praktična uporabnost
Predstavljen bo model, ki bo organizacijam v pomoč pri vpogledu, vzpostavitvi informacijske varnosti in zaščiti pred kombiniranimi grožnjami, uporabi mobilnih naprav in povezovanja v oblak.

Izvirnost
Prispevek predstavlja temo, ki je trenutno za organizacije in uporabnike v veliki meri enigma. Viri o izbrani temi pa redkost.

Ključne besede: kombinirane grožnje, mobilne naprave, oblak

1 Uvod

Računalništvo v oblaku v sodobni IKT omogoča hitrejše delo, stalno dostopnost do podatkov, nižanje stroškov in obljublja višji nivo varovanja dostopa. Ideja oblaka ni nova, je pa zadnja leta izvedljiva s pomočjo naprednejših internetnih povezav in modernejše informacijske tehnologije. Računalništvo v oblaku lahko definiramo kot souporabo računalniških resursov preko interneta, kjer uporabnik za upravljane ne potrebuje veliko računalniškega znanja oziroma uporabniku preprosto ni potrebno skrbeti za upravljanje, njegova skrb je uporaba (Glavač, 2009). Naložbe v lastno informacijsko tehnologija so ob zakupu/nakupu oblaka načeloma manjše kot naložbe v klasično IT infrastrukturo. Tehnologija večinoma deluje avtomatično, zato lahko podjetje oz. organizacija zaposli manjše število informatikov. Hiter razvoj informacijske tehnologije in dostopnejše ter hitrejše internetne povezave nam omogočajo, da lahko s prenosnim telefonom pregledujemo vse pomembnejše novice dneva, opravimo poslovanje z banko, pregledamo elektronsko pošto, na voljo pa so nam še druge storitve.

Pa je res mogoče v vsakem trenutku priti do podatkov v oblaku? Kako je z varnostjo in zasebnostjo le-teh? Pri stalnosti dostopa do podatkov izven fizičnih meja organizacije so nam v veliko pomoč mobilne naprave (naprave, ki se s pomočjo brezžičnih, mobilnih ali »Bluetooth« omrežij povezujejo v splet (Rupnik, Krisper, 2010)) in različna, predvsem javna omrežja, ki nam omogočajo dostop do oblaka ali informacijskega sistema organizacije z namenom pregleda ali prenosa podatkov, elektronske pošte, ali dela z aplikacijami.

Velika količina podatkov, ki je na voljo v vsakem trenutku, je shranjena v korporativnih informacijskih centrih in/ali v računalniškem oblaku. S pomočjo mobilnih naprav in pripadajoče programske opreme enostavno dostopamo do poslovnih podatkov (elektronske pošte, dokumentov, podatkovnih baz ipd.), saj je zaradi hitrosti poslovnih procesov, konkurence in sprejemanja pomembnih odločitev nujno imeti hiter in učinkovit dostop do informacij. Pomembno je tudi poskrbeti za informacijsko varnost, saj so od tega odvisni razpoložljivost in integriteta podatkov ter zaupanje v informacije, poslovne procese in odločitve, ki jih sprejema in predstavlja organizacija.

Zamisel oblaka kot storitve informacijske tehnologije izvira še iz časov terminalov in zaprtih, med seboj nepovezanih podjetniških omrežij. S hitrim razvojem tehnologije prenosa podatkov po različnih omrežjih in mobilnih napravah, predvsem pa zaradi visokih stroškov nakupa informacijske tehnologije in storitev, je zamisel računalništva v oblaku vnovič oživela. Podjetja se čedalje pogosteje odločajo za oblak zaradi enostavnosti in ker jih je gospodarska kriza prisilila k zmanjševanju stroškov informatike. Podjetja oblak, kjer uporabljajo storitve informacijske tehnologije in sistema, vidijo kot priložnost zmanjšanja stroškov nakupa in vzdrževanja lastne informacijske tehnologije ter dostopa do vedno novejših različic programske opreme (Rodier, 2011).

Elektronska pošta, odlaganje dokumentov, podatkovne baze in dodatna nadomestna lokacija so le nekatere storitve, ki jih nudijo kot storitev v oblaku. Zaradi večje prilagodljivosti storitev in informacijske varnosti, glede na želje organizacij, so storitve oblaka razdeljene na tri dele; javni, hibridni in privatni oblak. Podjetja lahko s svojimi informatiki in varnostnimi metodami (gesla, enkripcija podatkov, redundanca ipd.) skrbijo za lasten, zasebni oblak. Ta se navadno nahaja znotraj korporativnega omrežja, medtem ko za javni oblak ne poznamo natančne fizične lokacija – nahaja se pač nekje na internetu. Iz povedanega sledi, da prenos podatkov v oblak lahko predstavlja dodatno informacijsko tveganje. Javni oblak nam omogoča, da lahko podjetje ali organizacija prenese vse svoje potrebe po informacijski tehnologiji na internet. Hibridni oblak je kombinacija zasebnega in javnega oblaka. Pomembni podatki so shranjeni v zasebnem oblaku znotraj korporativnega omrežja, medtem ko izkoriščajo programsko opremo

javnega oblaka (Glavač, 2009). Od vrste oblaka in načina zavarovanja in dostopa pa je odvisna tudi varnost naših podatkov.

2 Oblak, mobilne naprave in programske oprema za dostopanje

Organizacije se odločajo za prenos podatkov v oblak, ker s tem zmanjšajo stroške informacijske tehnologije in vzdrževanja. Z zakupom pridobijo prostor, storitve, programsko opremo, redundanco lastnih podatkov in dostopnost v vsakem trenutku za nižjo ceno glede na klasično IT infrastrukturo. Poleg pozitivnih stvari pa se pojavlja vprašanje informacijske varnosti. Ponudniki storitev oblaka zagotavljajo varnost po principu zasebnosti in zaupnosti. Kdo vse lahko dostopa do informacij, ki jih damo v oblak, in kje natanko so naši podatki oz. del oblaka z našimi podatki, pa ni natančno določeno. Možno je, da do njih dostopajo nepooblaščene osebe, tekmeci, obveščevalne službe, ... Organizacije so pri dostopu do oblaka odvisne od kakovosti in hitrosti internetne povezave; hiter in zanesljiv dostop pa je predpogoj za uporabo javnega ali hibridnega oblaka. Ob tem se moramo vprašati tudi o kakovosti redundance in ali je zares zagotovljeno neprekinjeno delovanje oblaka, kar vpliva na dostopnost podatkov v njem. Kako je v pravnem smislu urejen vidik lastništva vsebin v oblaku? Poskrbeti je potrebno poskrbeti za redundanco naših podatkov in zagotoviti, da se v primeru, ko podjetje spremeni lastnika, podatkom nič ne zgodi (Brodkin, 2008).
Hitremu razvoju velikih sistemov, predvsem prenosu podatkov v oblak, sledi tudi razvoj mobilnih naprav in programske opreme zanje (Weber, Darbellay, 2010). V zadnjem obdobju izstopa veliko povečanje uporabnikov mobilnih telefonov in tabličnih računalnikov (Chicone, 2009; Riedy in drugi, 2011). Ker so te naprave zelo funkcionalne in imajo napredno programsko opremo ter dostop do storitve, ki jih omogoča oblak, so začele nadomeščati osebne računalnike. Če imamo dostop do interneta, so nam s pomočjo mobilne naprave v vsakem trenutku dostopne storitve kot so elektronska pošta, splet, pomembni poslovni podatki, ... Sistem je z uporabniškega vidika enak kot v primeru povezovanja v informacijsko okolje organizacije s pomočjo mobilne naprave. Razlika je v tem, da je tveganje večje, ko dostopamo v hibridni ali javni oblak. Programska oprema na mobilnih telefonih pri dostopu do podatkov v oblaku lahko deluje zgolj kot uporabniška aplikacija, ki samo prikazuje podatke, medtem ko za analizo poizvedb skrbi programska oprema v oblaku. Primer je uporaba aplikacij, ki delujejo na osnovi podatkovnih baz, pri kateri se vse poizvedbe po informacijah generirajo v oblaku nekega podjetja ali organizacije, končni rezultati pa se prenesejo in prikažejo na mobilni napravi. Strokovnjaki ugotavljajo, da napreduje razvoj programske opreme s svetlobno hitrostjo, pozablja pa se na standardiziranje in certificiranje programske opreme. Ta pomanjkljivost se kaže tako na strani izdelovalcev kot uporabnikov. Programska oprema na mobilnih napravah zato lahko deluje nenadzorovano. Pri povezovanju v omrežje z mobilno napravo najpogosteje ne vemo, kaj se v njej dogaja. Z uporabo nepreverjene, nestandardizirane programske opreme lahko nevede odpremo vrata svojega poslovnega informacijskega sistema ali oblaka in s tem povečamo tveganje, da nam odtujijo podatke, to pa ogrozi integriteto in delovanje celotne organizacije (Saksida, 2008).

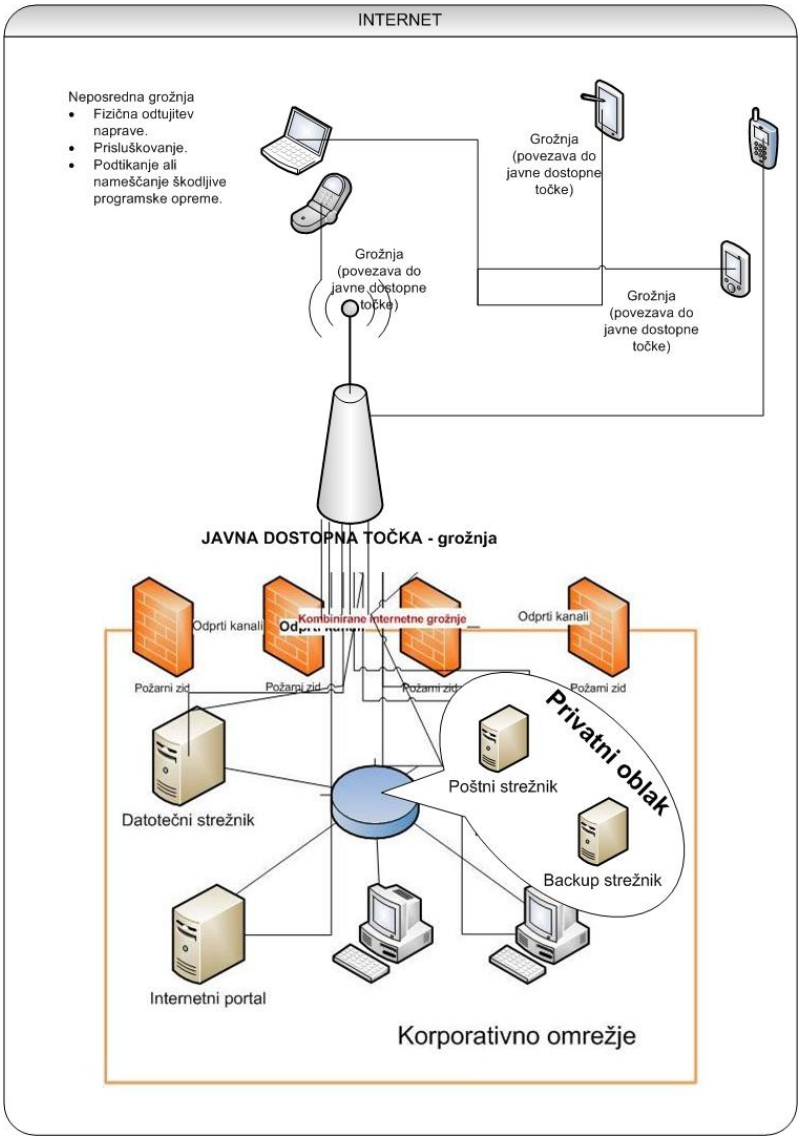
3 Varnost dostopa do oblaka z mobilnimi napravami in obramba pred grožnjami

Najšibkejši člen informacijske varnosti v podjetju ali organizaciji sta uporabnik in njegova stopnja poznavanja tehnologij, ki jih uporablja. Z nezavedno uporabo mobilnih naprav in njihove programske opreme lahko uporabnik ogrozi delovanje celotne organizacije.

Ugotavljamo, da je pomembno poskrbeti za ustrezne standarde, ki določajo vrsto izročenih sredstev v organizaciji in pravila njihove uporabe. Obenem je potrebno v organizaciji poskrbeti za ustrezno izobraževanje uporabnikov, predvsem iz vidika zavedanja o možnih grožnjah in njihovih posledicah (European Network and Information Security Agency – ENISA, 2010). Zaposlene je zato potrebno stalno izobraževati o nevarnostih uporabe mobilnih naprav in njihovi odgovornostih v primeru, da (vede ali nevede) povzročijo varnostni incident in škodo organizaciji. Cilj organizacije pa je zagotavljanje varne rabe izročenih sredstev. 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, se zelo zmanjšajo vplivi groženj. Ugotovimo torej lahko, da je potrebno postaviti izhodišča za standardizacijo izročenih sredstev, ter s tem zagotoviti boljšo informacijsko varnost (Bernik, Prislan, 2010).

Z varnostnega stališča je uporaba oblaka v poslovnem sistemu dodatno informacijsko tveganje in izpostavljanje grožnjam, ki lahko delujejo posamično ali skupno, posredno ali neposredno. Kot primer neposredne grožnje lahko navedemo fizično odtujitev mobilne naprave, medtem ko so posredne grožnje mnogo bolj sofisticirane in nepredvidljive – in se je pred njimi veliko težje zavarovati. Npr. ko se uporabnik povezuje v korporativno informacijsko okolje s pomočjo mobilne naprave in javnega omrežja, se grožnje pojavljajo na mnogih segmentih (mobilne naprave, internetna povezava od mobilne naprave do informacijskega sistema organizacije z vsemi vmesnimi dostopnimi točkami, predvsem so rizična javna omrežja in javno dostopne točke, programska oprema, ki deluje nenadzorovano...) 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). Gre za skupek različnih elementov, ki ogrožajo varnost informacijskega sistema. Ko se povežejo različni elementi, lahko »prelisičijo« obstoječo informacijsko varnostno opremo, ki v večini primerov ni kos kombiniranim grožnjam. Z napadom na informacijski sistem, ki poteka na več ravneh – prva raven je lahko popolnoma preprosta programska oprema, ki si jo uporabnik namesti na mobilno napravo in jo naša zaščita ne zazna kot nevarnost, lahko pride do odtujitve podatkov oz. velike materialne škode. Sodobne varnostne rešitve, ki jih uporabljajo organizacije, ne zadoščajo za ustrezno varovanje informacijskega sistema in njegovih delov pred grožnjami, ki jih predstavljajo mobilne naprave.

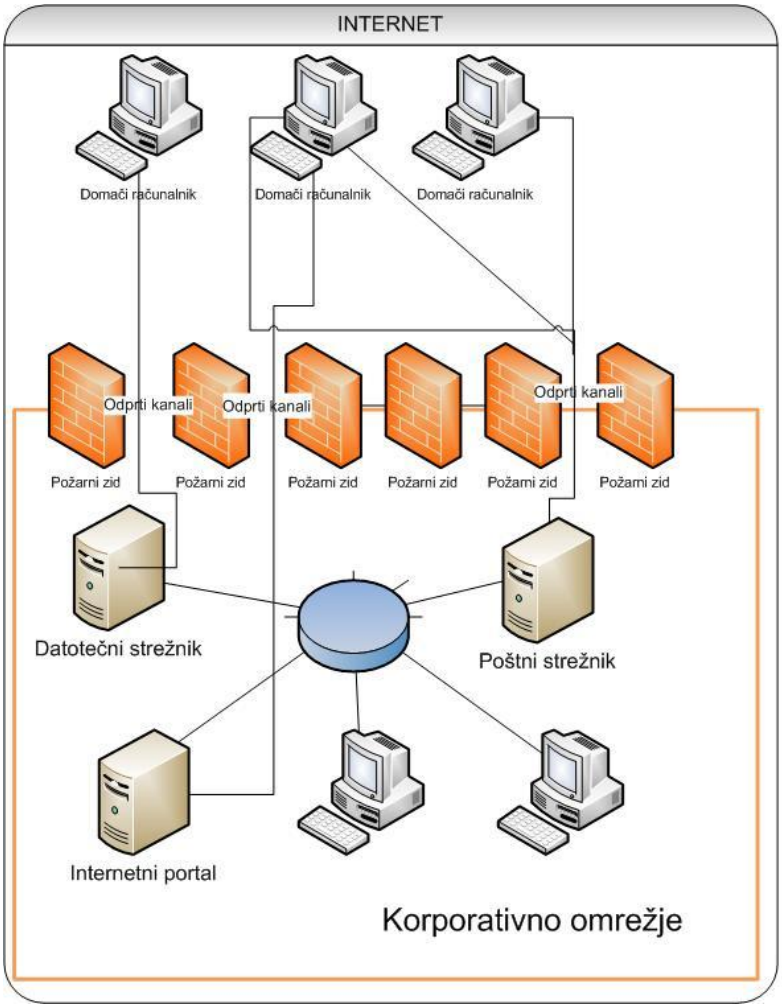
Slika 1 prikazuje centralni informacijski sistem organizacije v katerem se nahaja tudi privatni oblak. Kot smo že omenili je privatni oblak navadno integriran znotraj informacijskega sistema in je v popolnem nadzoru dotične organizacije in je lahko v popolni lasti korporacije ali v najemu od nekega zunanjega ponudnika, ki tudi skrbi za vsa popravila in težje odprave napak. Uporabniki se z svojimi mobilnimi napravami povezujejo skozi javno omrežje v informacijski sistem organizacije. Ker nadzor poti komunikacije med mobilno napravo in informacijskim sistemom organizacije ni učinkovit, so sistemi in naprave posledično izpostavljene različnim grožnjam. Te so lahko posredne (fizična odtujitev naprave, prisluškovanja in prestrezanja komunikacij) ali neposredne (napadi so bistveno bolj nepredvidljivi in se pred njimi ni moč stoodstotno zaščititi). Slika 2 prikazuje javni oblak, ki ga je zakupila organizacija za svoje potrebe. Tukaj se že oblak lahko smatra kot potencialna grožnja. Ravno tako kot pri sliki ena je možnosti za vdor v sistem veliko, grožnje so lahko samostojne ali delujejo simultano. Vendar se možnost vdora oziroma odtujitve informacij bistveno poveča, ker imamo dva sistema ki sta lahko potencialni točki napada, predvsem tisi v privatnem oblaku predstavlja zaradi »oddaljenosti« šibkejši točko.



Slika 1 : Komunikacija centralnega informacijskega sistema s mobilnimi napravami in komunikacija mobilnih naprav s spletom ter uporaba privatnega oblaka.

Organizacije zmanjšujejo tveganje z implementacijo strojne opreme, ki pregleduje potencialne nevarnosti na ravni internetnega prometa (Whitman, Matorord, 2008), ter s posebnimi napravami, ki skrbijo za preprečevanje vdorov v sistem (Scarfone, Mell, 2007). Nekatera podjetja, ki skrbijo za razvoj varnostne programske opreme, že nudijo napredno varnostno programsko opremo za mobilne naprave (Schechtman, 2011) in programske požarne zidove, ki pregledujejo internetni promet tako na mobilnih napravah kot na centralnem domenskem sistemu (Endait, 2011). Tovrstna programska oprema organizacijam omogoča centralno uveljavljanje varnostnih pravil za mobilne naprave (Mottishaw, 2010). V sklopu pridobitve certifikata ISO 27001 so nekatere organizacije uveljavile interne pravilnike za zagotavljanje informacijske varnosti (npr. Calder, 2006; Bernik, Prislan, 2011), kar je posebej pomembno pri rabi mobilnih naprav. Prilagoditev pravilnikov, kot pomembnega dela zaščite informacijskega sistema pred grožnjami pri uporabi mobilnih naprav, je nujna. To je nujno zaradi vse večjega števila potencialno nevarne programske opreme, ki jo uporabniki samodejno nameščajo na

mobilne naprave. Pravilniki naj vsebujejo navodila za uporabo standardizirane, predhodno varnostno testirane programske opreme, in kaj doleti uporabnika, ki prekrši pravila. Standardi naj določajo, kako uporabljati programsko in strojno opremo in definirajo tudi protokole za varno mobilno povezovanje v centralna informacijska omrežja in organizacijski informacijski sistem.



Slika 2: Komunikacija centralnega informacijskega sistema s mobilnimi napravami in komunikacija mobilnih naprav s spletom, ter uporaba javnega oblaka.

4 Zaključek

Vedeti, kako pravilno in varno uporabljati mobilne naprave in storitve oblaka, ki so del informacijskega sistema podjetja ali organizacije, je lahko velika konkurenčna prednost v tekmi za prevlado v znanstvenem in gospodarskem okolju. Z zmanjševanjem možnosti za vdor v informacijski sistem, odtujitev in zlorabo informacij se krepi zaupanje v procese in informacije, s katerimi operiramo v določenem okolju, zato je nujno vzpostaviti varen dostop do informacijskega sistema organizacije. Razvoj različnih možnosti vzpostavljanja informacijske varnosti, gre v smeri pregleda internetnega prometa, šifriranja podatkov in podeljevanja certifikatov za dostop do zasebnih informacijskih sistemov. Najšibkejši člen informacijske

varnosti pa še vedno ostajajo uporabniki. Dodatno tveganje pa prestavljajo mobilne naprave, s katerimi dostopajo do podatkov, predvsem prek javnih omrežij, v centralni informacijski sistem neke organizacije. Zato je potrebno vzpostaviti standarde informacijske varnosti, ki natančno določajo načela varne uporabe mobilnih naprav, programsko opremo, ki jo je dovoljeno imeti na mobilnih napravah, in protokole varnega povezovanja v centralni informacijski sistem. Na ta način se zmanjša vpliv kombiniranih groženj in zagotovi višja stopnja varnosti korporativnih podatkov pri kombinaciji rabe mobilna naprava - javno omrežje - oblak.

5 Literatura

Bernik, I. in Prislan, K. (2010). Proces upravljanja s tveganji v informacijski varnosti. V P. Umek in T. Pavšič Mrevlje (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.

Brodkin, J. (2008). *Gartner: Seven Cloud Computing Security Risks*. Pridobljeno 27.4.2011 na www.infoworld.com.

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

Chicone, R. G. (2009). *An Exploration of Security Implementations for Mobile Wireless Software Applications within Organizations*. Minneapolis: Graduate Faculty of the School of Business and Technology Management, Northcentral University.

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 EU.

Glavač, Z. (2009). *Računalništvo v oblaku in virtualizacija* (Diplomsko delo). Maribor: Fakulteta za elektrotehniko, računalništvo in informatiko.

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.

Riedy, M. K., Beros, S. in Wen H. J. (2011). Management Business Smarthphone Data. *Journal of Internet Law*, 3-14.

Rodier, M. (2011). The Year Of Compliance And The Cloud. *Wall Street & Technology, 29*(2), 26.

Rupnik, R. in Krisper, M. (2003). Model kontekstno odvisnih aplikacij. *Uporabna informatika, 11*(3), 122-130.

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

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.

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

Weber, A. in Darbellay, A. (2010). Legal Issues in Mobile Banking. *Journal of Banking Regulation, 11*(2), 129-145.

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