Učinki stalnega dostopa v kibernetski prostor in odtujevanje podatkov

Blaž Markelj, Igor Bernik

Potreba po hitrem odločanju v poslovnem in zasebnem okolju, vsiljuje potrebo po stalnem dostop do podatkov. Pri odločanju je možnost neprestanega dostopa nujna za konkurenčnost. Z mobilnimi napravami je stalen dostop enostaven, internetne povezave, računalništvo v oblaku in pripadajoča programska oprema, pa povezuje potrebne elemente dostopa in predstavitve podatkov. Raznovrstna programska oprema na mobilnih napravah omogoča hiter in enostaven dostop do shranjenih podatkov. S pomočjo mobilne naprave smo z internetom lahko povezani stalno, to pa omogoča dostop do potrebnih podatkov, ne glede na to, kje se nahajajo. Pa naj bo to znotraj informacijskega sistema ali v oblaku. Ob vseh prednostih in nenehnih novostih, ne smemo pozabiti na številne grožnje, ki pri dostopu pretijo uporabnikom mobilnih tehnologij. S hitrim razvojem mobilnih tehnologij so se zaradi zapostavljanja varnosti razvile številne grožnje. Ugotovitve globalnih organizacij na podlagi analiz groženj mobilnim napravam kažejo veliko povečanje teh. Glavni izvor groženj je, poleg prenosljivosti naprav, raznolika in varnostno nepreizkušena programska oprema. Za ugotavljanje stanja v slovenskem prostoru in možnosti boljšega odkrivanja zlorab, smo izvedli raziskavo, ki kaže na stopnjo zavedanja odtujevanja podatkov pri rabi mobilnih naprav; na podlagi rezultatov predlagamo rešitve za zmanjšanje tveganj in boljše zaščite podatkov, ob morebitni zlorabi pa možnosti odkrivanja storilcev.

Ključne besede: informacijska varnost, kombinirane grožnje, mobilne naprave, računalniški oblak, zavedanje

1 Uvod

Novitete na področju mobilnih naprav so namenjene pomoči dostopanja do potrebnih podatkov za hitro in kakovostno odločanje. Zato je bistvenega pomena, da je dostop hiter in stalen. Razvoj interneta, mobilnih naprav, računalništva v oblaku in pripadajoče programske opreme so zagotovili stalen dostop do podatkov, ne glede na kraj in čas sprejemanja odločitev. Spreminja se načini hranjenja in obdelovanja podatkov. Čeprav ideja računalništva v oblaku ni nova, je zdaj uresničljiva zaradi razvoja tehnologij (internetnih povezav, strežniških sistemov itd.) povezovanja in hranjenja podatkov, kar omogoča transparenten stalen dostop do podatkov. Za kakovostno odločanje je smiselno podatke hraniti tako, da dostopamo do njih z uporabo mobilnih tehnologij in prenosa podatkov transparentno, brez posebnega znanja. Raziskava, ki jo je objavila organizacija comScore (2011), je pokazala, da je v novembru 2011 internet uporabljalo že 380 milijonov Evropejcev. Pri tem bo, po ugotovitvah MicrostoftTag (2011), do leta 2014 število mobilnih dostopov do interneta preraslo dostope izvedene z namiznimi računalniki, že danes pa se to razmerje približuje 50 odstotkom. S pomočjo mobilnih naprav in stalnega dostopa do interneta dejansko neprestan dostop do podatkov pride do izraza,. Saj mobilne naprave predstavljajo povezovalni element oz. stično točko med uporabnikom in mestom hranjenja podatkov.

Vendar pa so učinki stalnega dostopa lahko tudi negativni. Tako so uporabniki mobilnih naprav lahka tarča številnih groženj, ki delujejo z namenom zlorabe njihovih podatkov. Grožnje se lahko uresničijo s pomočjo številnih zlonamernih kod, prestrezanja komunikacije ali zgolj zaradi odtujitve naprave. Številna svetovna podjetja, ki se ukvarjajo z izdelavo zaščitne programske opreme, poročajo o velikem povečanju števila raznovrstnih virusnih

okužb, poznavanje naše GPS lokacije, prenos in zloraba osebnih podatkov (certifikati, gesla itd.) ter avtomatične vključitve posameznih delov programske kode. To so le nekatere zlorabe, ki se vse pogosteje izvajajo na mobilnih napravah.

Da zlorabe preprečimo, pa moramo poznati postopke (včasih tudi delovanje programske in strojne opreme) in v primeru zlorab ustrezno ukrepati, da zaščitimo (še) ne odtujene podatke, v nadaljevanju pa zlorabo prijaviti pristojnemu CERT-u in drugimi ustreznim organom. Uporabniki bi moral ob sumu kaznivega dejanja nemudoma obvestiti pristojne organe, saj je potem pridobitev in ohranitev ustreznih dokazov ter digitalnih sledi bistveno boljša, pri tem pa smiselno upoštevati postopke pridobivanja digitalnih dokazov, ki jih določa Zakon o kazenskem postopku [ZKP-UPB4] (2007) z 219.a in 223.a členom. V poslovnih sistemih se je smiselno izobraziti zaposlene in nanje prenesti postopke varnosti in zavarovanja digitalnih dokazov v primeru zlorab za učinkovitejše odzivanje in odkrivanje napadov in napadalcev.

Informacijska infrastruktura, kjer so shranjeni podatki, mora biti prilagojena oddaljenim dostopom, torej primerno zavarovana. V preteklosti so se za namene oddaljenega dostopa v požarnih zidovih puščali odprte specifična vrata v sistem, po katerih je potekala komunikacija oddaljenega dostopa – RDP[1]. Sodobne mobilne naprave pa se neposredno povezujejo z internetom, zato večina informacijskih tokov poteka na splošni način (http[2]), ki je namenjen spletni komunikaciji (brskanje), zato so vrata na požarnem zidu že v osnovi odprta in nezavarovana, s čimer se poveča ogroženost.

Poleg hranjenja podatkov v lastni informacijski infrastrukturi, vse več uporabnikov podatke hrani in/ali obdeluje v računalniškem oblaku. Ker tehnologija v oblaku deluje na virtualni ravni z avtomatiziranimi sistemi, to pomeni, da je dodeljevanje virov stvar avtomatike sistema. Tako je potrebno zagotoviti ustrezno obrambo pred grožnjami, v primeru zlorab podatkov pa za ustrezno digitalno dokazovanje zlorab in pregon storilcev kibernetskega kriminala, kar je zaradi oddaljene (in pogosto nepoznane) lokacije zahtevno, previdnost pa velja tudi pri izbiri ponudnika oblaka. Smernice kažejo, da se uporaba računalništva v oblaku z leti povečuje, s tem pa tudi tveganja. Podjetje TechNavio je objavilo poročilo o trenutni razširjenosti storitev računalništva v oblaku in predvidevanja prihodnje rasti teh storitev. Pričakuje se 42 odstotno rast med letoma 2010 in 2014 (Infiniti Research Limited, 2011).

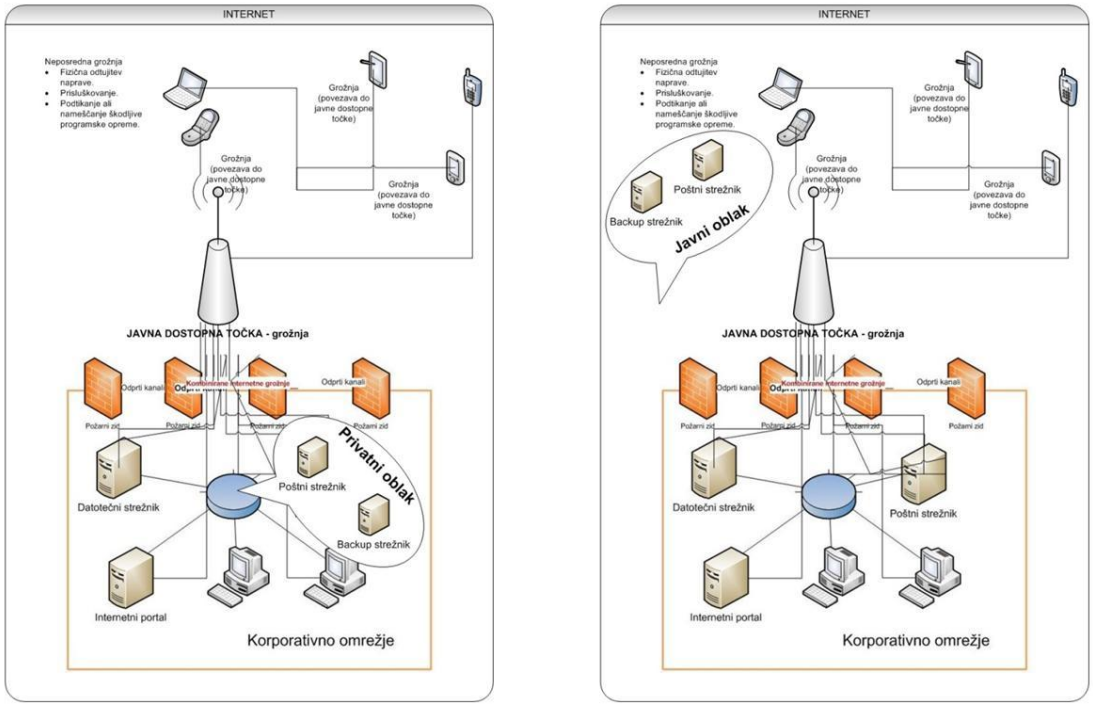
1.1 Grožnje mobilnim napravam, dostopu in informacijam

Najšibkejši člen v celotnem procesu prenosa in hranjenja podatkov predstavljata uporabnik ter njegovo znanje o varni uporabi mobilnih naprav, oblaka, programske opreme in prenosa podatkov. V zadnjem obdobju lahko spremljamo veliko povečanje raznovrstnih okužb mobilnih naprav. Organizaciji Lookout (2011) in Juniper (2011) v poročilih navajata veliko povečanje okužb mobilnih naprav s škodljivo programsko opremo. Postavlja se vprašanje, zakaj bi nekdo želel vdreti v informacijski sistem organizacije ali oblak, ko pa lahko vse podatke pridobi s pomočjo mobilne naprave, saj se večina mobilnih naprav povezuje v te sisteme prek raznovrstnih omrežij. Ker se število naprav stalno povečuje, narašča tako število groženj kot število zlorab. Za primer naj navedemo, da raziskava IDC-ja (2011) ugotavlja, da se v svetovnem merilu prodaja pametnih mobilnih telefonov povečuje za 55 odstotkov na leto. Po raziskavi CEE Telco Industry Report, ki jo je izvedla organizacija GfK Group (2011) (zajela je 15 držav Srednje in Vzhodne Evrope), je Slovenija po uporabi pametnih mobilnih telefonov vodilna, saj kar 27,8 odstotkov uporabnikov mobilne telefonije uporablja pametni mobilni telefon, sledijo ji Turčija z 23,7 odstotka in Litva z 18,5 odstotki. S povečanjem

[1]Remote Desktop Protocol (Povezava z oddaljenim namizjem) (TechTarget, 2007).
[2]Hyper Text Transfer Protocol (glavna metoda za prenos informacij po internetu) (Presentia, 2010).

števila uporabnikov mobilnih naprav se povečuje izpostavljenost, napredujejo grožnje, zaradi omenjenega pa se število primerov kibernetske kriminalitete, zaradi pričakovanega večjega izplena, povečuje.

Kot rečeno, so lahko podatki, do katerih dostopamo z mobilnimi napravami, na več različnih lokacijah, zato je treba razdelati grožnje in zagotoviti ustrezno zaščito. Grožnje lahko delujejo na več delih ter posamično ali kombinirano (Markelj in Bernik, 2011), večinoma pa z namenom odtujitve podatkov. Identificirati je potrebno mesta, na katerih se lahko pojavijo grožnje, ugotoviti vrste groženj in možnosti zlorab.



Slika 1: Grožnje pri dostopanju do informacijskega sistema organizacije ali oblaka

Slika 1 prikazuje možne grožnje, ko uporabnik mobilne naprave dostopa do podatkov znotraj informacijskega sistema organizacije ali oblaka. Prikazane so relacije med uporabnikom, mobilnimi napravami in centralnim informacijskim sistemom in oblakom. Na posameznih relacijah so predstavljene morebitne grožnje, vendar se je potrebno zavedati, da te (kot je predstavljeno na sliki) velikokrat, z namenom hitrejše in učinkovitejše odtujitve podatkov, delujejo kombinirano (skupaj in istočasno).

Informacijski sistem organizacije in računalniški oblak sta posredno ogrožena zaradi uporabe mobilne naprave in (odprtega) dostopa do podatkov, posebej v primerih, ko ne uporabljamo potrebnih varnostnih mehanizmov (avtentikacije, enkripcije, tunelnega protokola, varnih internetnih povezav in dostopov). Beckham (2011) navaja pet najbolj izpostavljenih informacijsko-varnostnih tveganj pri uporabi računalništva v oblaku, ki jih potencira uporaba mobilnih naprav. Na prvem mestu je prenos podatkov med informacijskim sistemom organizacije, uporabnikom (oz. mobilno napravo) in oblakom. Izpostavljeno je tveganje prenosa podatkov skozi več različnih ponudnikov interneta in hkrati neuporaba enkripcije podatkov, avtentikacije in varne internetne povezave (https ipd.). Na drugem mestu so varni programski vmesniki, kar je povezano s tem, kako se uporabniki avtenticirajo za dostop do podatkov v oblaku. Sledijo dileme glede varnosti hranjenih podatkov, njihove razpršenosti in enkripcije. So podatki stalno kriptirani, tudi v času prenosa do aplikacije prikaza in hranjenja

na strežniku? Veliko informacijsko varnostno tveganje predstavlja odvisnost od neprestanega dostopa in s tem odvisnosti od internetnih povezav.

2 Metoda

Decembra 2011 je bila med študenti izvedena raziskava o poznavanju in zavedanju groženj uporabnikov mobilnih naprav. Spletni vprašalnik je bil objavljen tri tedne na spletnem portalu »1ka« (www.1ka.si). Zbrane podatke smo analizirali s programom SPSS; ugotavljali smo tipe uporabnikov in namen uporabe mobilnih naprav ter najpogostejše vrste uporabljenih mobilnih naprav in programskih rešitev, ocenili poznavanje in uporabo varnostnih rešitev ter poznavanje in zavedanje groženj, ki pretijo ob uporabi mobilnih naprav. Obravnavali smo 281 izpolnjenih vprašalnikov. Ker nekateri vprašalniki niso bili izpolnjeni v celoti, se je pri posameznih vprašanih vzorec populacije spreminjal.

		N	%
Starost (n=281)	do 20 let	75	26,7
	od 21 do 25 let	133	47,3
	od 26 do 34 let	57	20,3
	od 35 do 44 let	2	4,6
	od 44 do 54 let	2	0,7
	Več kot 55 let	1	0,4
Spol (n=275)	Ženske	169	61,5
	Moški	106	38,5
Izobrazba (n=280)	srednja šola	177	63,2
	1. bolonjska stopnja	67	23,9
	2. bolonjska stopnja	25	8,9
	3. bolonjska stopnja	11	3,9

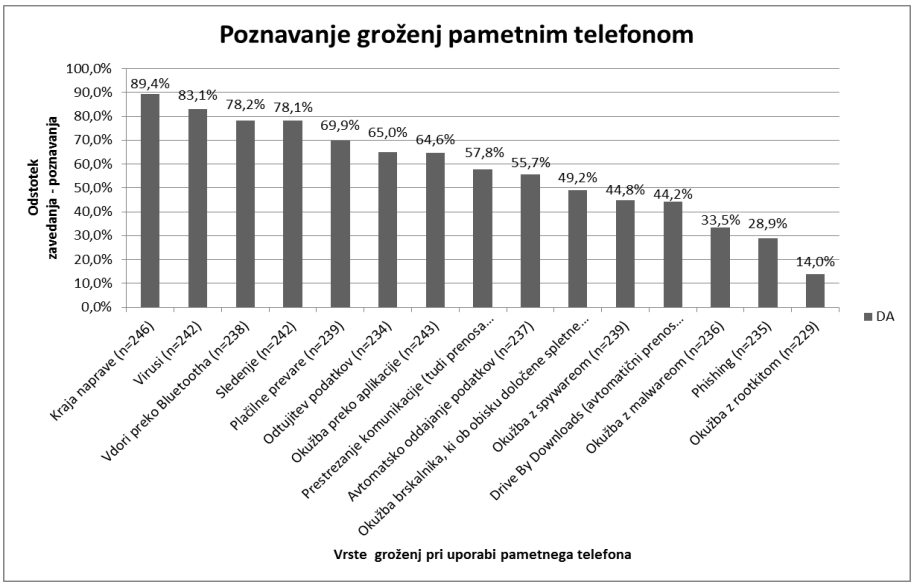
Tabela 1: Značilnosti vzorca anketiranih uporabnikov svetovnega spleta

Med vprašanimi je bila večina starih od 21 do 25 let, sledi starostna skupina do 20 let. Med vprašanimi je bilo 61,5 odstotkov žensk in 63,2 odstotka takih, ki imajo že zaključeno srednješolsko izobrazbo (Tabela 1).

3 Raziskava: varnostni vidik načina rabe mobilnih naprav

Podatki iz raziskave nam pokažejo, kako študenti uporabljajo mobilne naprave in dostopajo do kibernetskega prostora. Cilj raziskava je prikazati, v kolikšni meri študenti poznajo grožnje (katerih posledice so odtujitev podatkov) in varnostne rešitve, ki jih lahko zaščitijo pred takšnimi zlorabami.

Slika 2 prikazuje grožnje, ki jih vprašani poznajo in se jih pri uporabi mobilnih naprav bojijo. Med najbolj prepoznavnimi grožnjami je kraja (89,4 %), sledijo virusi (83,1 %). Ti podatki ne presenečajo, saj so to grožnje, ki so poznane že dalj časa.



Slika 2: Poznavanje groženj pametnim telefonom

Zaskrbljujoče je dejstvo, da vprašani zelo slabo poznajo napredno škodljivo programsko opremo, katerih količina in načini delovanja se nenehno povečujejo. Medtem ko velike organizacije mesečno objavljajo rezultate analiz, ki nakazujejo veliko povečevanje števila okužb mobilnih naprav s škodljivo programsko opremo, smo v raziskavi ugotovili, da je poznavanje tovrstnih groženj slabo.

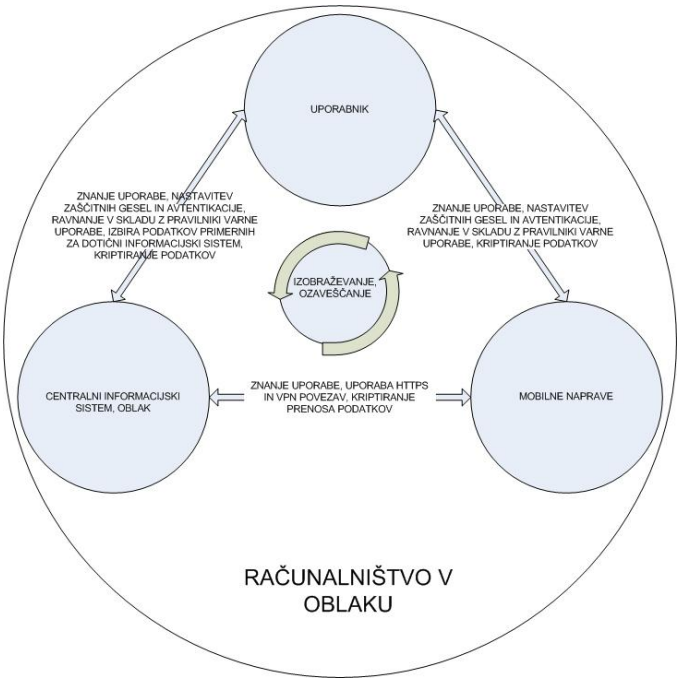
	Uporabljam		Poznam, vendar ne uporabljam		Ne poznam	
	N	%	N	%	N	%
Centralni nadzor pametnega telefona (določanje politike uporabe) (n=205)	13	6,3	83	40,5	109	53,2
Oddaljeno brisanje vsebin (n=206)	14	6,8	84	40,8	108	52,4
VPN povezava (n=206)	14	6,8	84	40,8	108	52,4
Avtentikacija ob uporabi določenih funkcij (n=208)	27	13	90	43,3	91	43,8
Enkripcija podatkov (n=206)	12	5,8	112	54,4	82	39,8
Arhiviranje vsebin pametnega telefona (n=205)	40	19,5	91	44,4	74	36,1
Izobraževanje (n=204)	53	26	84	41,2	67	32,8
Omogočeno sledenje pametnega telefona v primeru kraje (n=207)	42	20,3	104	50,2	61	29,5
PIN zadostop do aplikacij na pametnem telefonu (n=206)	44	21,4	117	56,8	45	21,8
Anti virusna zaščita (n=207)	61	29,5	102	49,3	44	21,3
PIN za SIM kartico (n=212)	190	89,6	21	9,9	1	0,5

Tabela 2: Uporaba varnostnih zaščit na pametnem mobilnem telefonu

Tabela 2 prikazuje nekatere možne rešitve za zavarovanje mobilne naprave pred grožnjami. Vprašani v največji meri uporabljajo standardno zaščito kot so PIN-koda za SIM-kartico in anti-virusne programe, medtem ko bolj naprednih orodij, kot sta enkripcija podatkov in oddaljeno brisanje vsebin z naprave sploh ne poznajo. Poznajo pa nekatere rešitve, kot je PIN-koda za dostop do posameznih aplikacij, vendar jih ne uporabljajo.

4 Diskusija o načinih implementacije in možnih rešitvah

Na trgu najdemo mnogo programskih rešitev, ki zavarujejo mobilno napravo, prenos podatkov in preprečijo možnosti okužbe s škodljivo ali vohunsko programsko opremo. Poznavanje uporabe strojne in programske opreme, pretečih groženj in možnosti zaščite je bistvenega pomena za, s stališča informacijske varnosti, varno uporabo mobilnih naprav. Slika 3 predstavlja oblike zaščite pri uporabi mobilnih naprav in dostopu do informacijskega sistema in/ali v oblaku shranjenih podatkov. Prikazane so možne rešitve na posameznih relacijah, v samem središču pa sta znanje in ozaveščenost. Slika 3 je nastala na podlagi spoznanj, ki smo jih dobili iz končnih rezultatov raziskave, ki smo jo izvedli med študenti, in na podlagi teoretičnih spoznanj. Dejstvo je, da mladi slabo poznavajo grožnje informacijski varnosti in varnostne rešitve, zato je kljub nekaterim dobrim tehničnim rešitvam težko preprečiti zlorabe mobilnih naprav in posledično možnosti odtujitve podatkov. S tem namenom smo v središče slike 3 postavili izobraževanje in ozaveščanje. Vse uporabnike mobilnih naprav je potrebno ozavestiti o grožnjah in potencialnih posledicah ter jih seznaniti z možnimi rešitvami.



Slika 3: Možne oblike zaščite na povezavah med mobilnimi napravami in centralnim informacijskim sistemom in/ali oblakom

Istočasno pa je potrebno, pred implementacijo oz. spremembo neke storitve, procesa ali organizacijske strukture, upoštevati različne vidike informacijske varnosti (D'Aubeterre, Singh in Iyer, 2008). Hkrati je dobro, da pri vpeljavi nove tehnologije ali spremembah obstoječe, sodelujejo med seboj vsi oddelki organizacije, saj se lahko le tako optimizirajo vsi sistemi in se zagotovi najvišja raven informacijske varnosti (Kietzmann, 2008).

Navedene ugotovitve na podlagi raziskav nam nakazujejo trend rasti groženj, ki pretijo uporabnikom mobilnih naprav in posledično tistim, ki uporabljajo stalni dostop do korporativnih podatkov. Na trgu se pojavljajo različne tehnične zaščite, ki pomagajo preprečiti odtujitev podatkov ali uresničitev posameznih groženj, le uporabiti jih je potrebno. Kot omenjeno, ima veliko mobilnih naprav že nameščena nekatera zaščitna orodja, ki pa jih uporabniki velikokrat ne uporabijo. Vsekakor je varnost odvisna od posameznikovega poznavanja tehnologije in védenja, kako jo uporabiti. Zato je potrebno ljudi ozavestiti, v organizacijah pa sprejeti potrebne pravilnike, ki definirajo uporabo mobilnih naprav, programske opreme in dostopanja do centralnega informacijskega sistema ter podatkov v oblaku. Oceniti je potrebno, kateri podatki so primerni za shranitev na mobilni napravi, v centralnem informacijskem sistemu in oblak ter seveda tudi, ali je do njih varno dostopati na daljavo. V primeru, da pride do zlorabe, je smiselno obvestiti pristojne organe, saj bodo ti ravnali v skladu s postopki, ki jim jih narekujeta osmi odstavek člena 219.a ZKP-UPB4 (2007) (ki govori o posebnem načinu zavarovanja podatkov) ter s tem zavarovali izvirnost in integriteto pridobljenih digitalnih dokazov (1. in 5. odstavek člena 223.a ZKP-UPB4, 2007). Forenzična preiskovanja digitalnih dokazov predstavljajo v svetu preiskovanja kriminalitete vse pomembnejši člen (Bernik in Prislan, 2012).

5 Zaključek

Načinov odtujitve podatkov je več. Vsem so zagotovo najbolj poznani načini, kot so odtujitev naprave, razna prestrezanja komunikacij ali direktni vdori v sistem. Med njih lahko prištejemo

tudi vdore s pomočjo dešifriranja ali kraje gesel. Obstajajo pa še veliko bolj prefinjeni načini, ki s pomočjo okužb sistema s škodljivo programsko opremo pridobijo ustrezne podatke ali odprejo »zadnja vrata« sistemov. Primer predstavljajo okužbe mobilnih naprav, ki posledično neznancem avtomatično posredujejo osebne informacije uporabnika. Med temi informacijami so lahko tudi certifikati, raznovrstna gesla in lokacija uporabnika.

Mark Fischetti (2011) je izdelal tabelo najbolj pogostih načinov odtujitve podatkov. Na vrhu lestvice so razni vdori v računalnike in strežniške sisteme organizacije (16 %). Takoj lahko potegnemo vzporednice z raziskavami podjetij Lookout (2011) in Juniper (2011), ki nakazujeta veliko povečanje raznovrstnih okužb, ter raziskavo o poznavanju in zavedanju groženj, ter uporabi možnih rešitev, ki smo jo sami izvedli med mladimi. Vse tri raziskave očitno kažejo, da se s povečanjem morebitnih okužb s škodljivo programsko opremo posledično povečuje tudi možnost vdora v sistem. Na drugem mestu najpogostejših oblik odtujitve podatkov je neposredni zajem podatkov na spletu. V tem primeru lahko spet naredimo primerjavo z raznimi okužbami, saj je za potrebe dostopa do uporabnikovih podatkov na spletu potrebno poznati tudi uporabnikovo geslo za dostop do profilov oziroma shramb podatkov v oblaku. Zanimivo je tudi dejstvo iz naše raziskave, da so kraja in virusi na dnu lestvice najbolj znanih načinov odtujitve podatkov.

Raziskave ne nakazujejo zmanjšanja rasti groženj mobilnim napravam in posledično zlorabam ter odtujitvam podatkov, ravno nasprotno. Tega se v veliki meri zavedajo tudi proizvajalci informacijsko varnostnih produktov. Panožne smernice nakazujejo nadaljnji razvoj posameznih programskih sklopov, ki bodo dejavni ob prijavi uporabnika v sistem, ki se aktivira z geslom, in bodo skladni s sprejeto organizacijsko politiko informacijske varnosti. Istočasno pa se vsi zavedamo pomembnosti izobraževanja in ozaveščanja posameznikov o varni uporabi mobilnih naprav in previdnega dostopanja do podatkov. Rešitve varovanja podatkov gredo v smeri razumevanja groženj, znanja uporabe tehnologij in poznavanja varnostnih rešitev.

Viri

Beckham, J. (2011). *The Top 5 Security Risks of Cloud Computing.* Pridobljeno 30. 12. 2011 na http://blogs.cisco.com/smallbusiness/the-top-5-security-risks-of-cloud-computing.

Bernik, I. in Prislan, K. (2012). *Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem.* Ljubljana: Fakulteta za varnostne vede, Univerza v Mariboru.

comScore. (2011). In Europe, *Apple iOSEco system Twicethe Size of Android When Accounting for Mobile Phones, Tablet sand Other Connected Media Devices*. Pridobljeno 18. 2. 2012 nahttp://www.comscore.com/Press_Events/Press_Releases/2012/1/Nearly_50_Percent_of_Internet_Users_in_Europe_Visit_Newspaper_Sites.

D'Aubeterre, F., Singh, R. in Iyer, L. (2008). Secure activity resource coordination: empirical evidence of enhanced security awareness in designing secure business processes. *European Journal of Information Systems, 17,* 587-542.

Fischetti, M. (2011). Stolen data: How thieves get your identity and other information. *Scientific American,* (Oct.). Pridobljeno 30. 12. 2011 na http://www.scientificamerican.com/article.cfm?id=data-breach-how-thieves-steal-your-identity-and-information.

GfKGroup. (2011). *CEE Telco Industry Report 2011*. Pridobljeno 6. 2. 2012 na http://www.gfk.com/group/press_information/press_releases/008894/index.en.html.

IDC. (2011). *IDC – PressRelease.* Pridobljeno 10 .9. 2011 na http://www.idc.com/getdoc.jsp?containerId=prUS22871611.

InfinitiResearchLimited. (2011). *Global Cloud System Management Software Market 2010-2014.* Pridobljeno 7. 9. 2011 na http://www.marketresearch.com/Infiniti-Research-Limited-v2680/Global-Cloud-Systems-Management-Software-6458283/view-stat.

Juniper Networks.(2011). *Malicious Mobile Threats Report 2010/2011*.Pridobljeno 10. 9. 2011 na http://www.juniper.net/us/en/dm/interop/go.

Kietzmann, J. (2008). Interactive innovation of technology for mobile work. *European Journal of Information Systems, 17,* 305-320.

Lookout. (2011). *Lookoutmobilethreatreport*. Pridobljeno 10. 9. 2011 na https://www.mylookout.com/mobile-threat-report

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.

MicrosoftTag. (2011). *Infographic: Mobile Statistics, Stats&Facts 2011*. Pridobljeno 6. 2. 2012. na http://www.digitalbuzzblog.com/2011-mobile-statistics-stats-facts-marketing-infographic/.

Presentia. (2010). *Kaj je http?*. Pridobljeno 20. 3. 2012 na http://www.presentia.si/baza-znanja-helpdesk/2010/kaj-je-http/.

TechTarget. (2007). *Remote Desktop Protocol (RDP)*. Pridobljeno 20. 3. 2012 na http://searchenterprisedesktop.techtarget.com/definition/Remote-Desktop-Protocol-RDP.

Zakon o kazenskem postopku [ZKP-UPB4]. (2007). *Uradni list RS,* (32/2007, 68/2008, 77/2009, 91/2011).

O avtorjih

Igor Bernik, doktor znanosti, predavatelj in prodekan za izobraževalno dejavnost, Fakulteta za varnostne vede, Univerza v Mariboru.

Blaž Markelj, asistent za področje informatike in informacijske varnosti, Fakulteta za varnostne vede, Univerza v Mariboru.