Pogledi informacijske varnosti na storitve računalništva v oblaku

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

Namen prispevka:
Že nekaj let intenzivno spremljamo različne pristope, kako posameznikom in organizacijam približati storitev računalništva v oblaku. Skupaj s hitrim razvojem mobilnih naprav in učinkovitejšimi internetnimi povezavami je ta možnost postala realnost za veliko uporabnikov. Z nastopom svetovne gospodarske krize in zmanjševanjem stroškov za nakup in vzdrževanje informacijskih sistemov in opreme se storitev oblak zdi smotrna odločitev, vsaj za podjetja in druge organizacije. Uporabniki pa preslabo poznajo različne vidike informacijske varnosti ter njenega pomena pri implementacije in uporabi tako kompleksne storitve kot je računalništvo v oblaku. O informacijski varnosti je potrebno razmišljati že pri določitvi organizacijske strukture, novih procesih in seveda pri uvedbi novih tehnologij.

Metodologija:
Narejen je pregled raziskav in aktualnih virov na temo informacijske varnosti, groženj in vzpostavitvi storitve oblak tako na ravni organizacij kot individualnih uporabnikov. Osredotočili smo se tudi na načine dostopanja do podatkov in na mobilne naprave, ki se uporabljajo za prenos podatkov iz in v oblak.

Ugotovitve:
Storitev oblak je poznana že nekaj časa, vendar ne v takšni obliki kot se je uveljavila v zadnjih nekaj let. Razmeroma nov je predvsem način dostopanja. Organizacije si se danes morale zavedati dinamičnih elementov (mobilnih naprav), s pomočjo katerih uporabniki dostopajo do podatkov in aplikacij znotraj oblaka. Predvidevamo, da se organizacije še niso povsem začele zavedati obsega groženj, ki jim pretijo med uporabo računalništva v oblaku oz. dostopanju do oblaka z mobilno napravo.

Omejitve:
Prispevek obravnava temo, ki je trenutno zelo aktualna, vsaj sodeč po številu objavljenih prispevkov in napovedi prihodnje rasti računalništva v oblaku, bolj malo pa je bilo napisanega o informacijsko-varnostnih tveganjih računalništva v oblaku in grožnjah, ki pretijo pri dostopanju do podatkov ali aplikacij, predvsem pri uporabi mobilnih naprav.

Praktična uporabnost:
Predstavljena so nekatera informacijska tveganja, ki bi jih morali poznati podjetja, druge organizacije in posamezniki, preden se odločijo za računalništvo v oblaku. V središče smo zato postavili načine dostopanja do podatkov (predvsem dostop z mobilnimi napravami) in elemente informacijske varnosti hranjenja podatkov in neomejene dostopnosti. Bralec prispevka bo dobil celovit pregled dejavnikov tveganja, ki ogrožajo informacijsko varnost pri uporabi mobilnih naprav za dostopanju do storitev v oblaku.

Izvirnost:
Predstavljen je način obravnavanja groženj, ki pretijo informacijski varnosti pri uporabi mobilnih naprav za dostopanje do podatkov v oblaku. Organizacije in posamezniki se bodo teh groženj primorani zavedati in se podučiti, kako se lahko najbolje zavarujejo pred njimi.

Ključne besede: informacijska varnost, grožnje, mobilne naprave, dostop, oblak

1 UVOD

V zadnjem obdobju smo priča turbulentnemu razvoju informacijske tehnologije, predvsem segmentu računalništva v oblaku (Microsoft, Google, Apple idr.), mobilnih naprav (pametni telefoni, tablični računalniki) in napredne programske opreme za to tehnologijo. Skoraj vsaka mobilna naprava – natančneje, njena osnovna programska oprema – podpira različne možnosti povezovanja v splet, prenašanja podatkov in povezovanja do storitev, ki so na volj v oblaku. Računalništvo v oblaku predstavlja novo možnost shranjevanja in obdelovanja podatkov ter dostopanja do njih. Vsa tehnologija v oblaku deluje na virtualni ravni z avtomatiziranimi sistemi. To pomeni, da je dodeljevanje resursov stvar avtomatike sistema. Poznamo tri vrste računalništva v oblaku; pri prvi gre za zasebni oblak, ki je postavljen znotraj same informacijske infrastrukture organizacije; pri drugi gre za javni oblak, katerega lokacija nam ni znana – vemo samo, da je »nekje na spletu«; pri tretji pa govorimo o hibridnem oblaku, kombinaciji prvih dveh omenjenih možnostih. Smernice kažejo, da se uporaba računalništva v oblaku z leti povečuje. Podjetje TechNavio je objavilo poročilo o trenutni razširjenosti storitev računalništva v oblaku in predvidevanja prihodnje rasti teh storitev. Pričakujejo 42 odstotno rast med letoma 2010 in 2014 (Infiniti Research Limited, 2011). Vsekakor lahko v prihajajočih letih pričakujemo še večje premike tako pri računalništvu v oblaku kot tudi pri mobilnih naprave in programski opremi zanje. Slednja uporabniku na inovativen način omogoča boljši in preglednejši prikaz določenih podatkov. Ko uporabljamo številne možnosti novih tehnologija, pa največkrat pozabljamo na informacijsko varnost in ogrožajoče dejavnike. Tudi nevarnosti se namreč razvijajo inovativno in hitro. Poročilo, ki ga je objavilo podjetje Lookout (2011), nam prikazuje razraščanje groženj, ki spravljajo v nevarnost uporabnike mobilnih naprav, torej tudi vsem, ki imajo te naprave za dostopanje do podatkov v oblaku. Markelj in Bernik (2011) navajata, da grožnje mobilnim napravah lahko delujejo samostojno ali kombinirano, ter na različnih nivojih.

Smotrno je že na začetku, to je pri implementaciji ali spremembi neke storitve, procesov 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 optimalna raven informacijske varnosti (Kietzmann, 2008).

Pri vpeljavi računalništva v oblaku v večjo organizacijsko strukturo je pametno že na začetku, se pravi pri načrtovanju, upoštevati priporočila stroke za informacijsko varnost, in v procesu implementacije pritegniti k sodelovanju vse zaposlene, ki bodo ključni uporabniki novo uvedene tehnologije.

2 INFORMACIJSKO-VARNOSTNA TVEGANJA

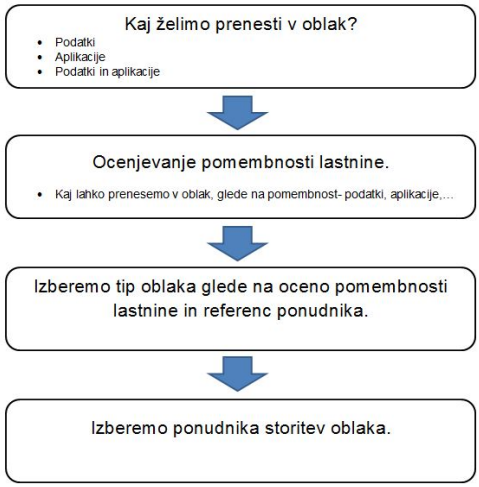
Beckham (2011) navaja pet najbolj izpostavljenih informacijsko-varnostnih tveganj pri uporabi računalništva v oblaku. Med njimi je na prvem mestu prenos podatkov med informacijskim sistemom organizacije, uporabnikom (npr. njegovo mobilno napravo) in oblakom. Izpostavljeno je tveganje prenosa podatkov, skozi več različnih internetnih ponudnikov in hkrati neuporaba enkripcije podatkov, ter avtentikacije in varnejše (npr. https) internetne povezave. Že na drugem mestu potem zasledimo varni programski vmesnik , kar pomeni na kakšen način se morajo uporabniki avtenticirati da lahko dostopajo do podatkov v oblaku. Sledijo varnostne dileme glede hranjenja podatkov, njihove razpršenosti in enkripcije. Ali so podatki ves čas enkriptirani, tudi v času prenosa do aplikacije in hranjenja na strežniku? Ne nazadnje predstavlja veliko informacijsko varnostno tveganje tudi odvisnost od neprestanega dostopa do informacija, kar pomeni da smo odvisni od internetnih linij, to predvsem pri javnem oblaku.

Mobilne naprave, predvsem pametni telefoni in tablični računalniki, so najhitreje razvijajoči se del informacijske tehnologije. Te naprave omogočajo neprestani dostop do spleta in s tem tudi povezavo z oblakom. Do javnega oblaka (Microsoft, Google, iCloud) imajo uporabniki neomejen brezplačni dostop že, ko odprejo osebni »računa«, organizacije pa morajo prostor v oblaku zakupiti. Z uporabo mobilnih naprav in groženj, ki jim pretijo, se posledično poveča tudi informacijsko varnostno tveganje za organizacije, ki uporabljajo računalništvo v oblaku in do svojih informacij dostopajo s pomočjo mobilnih naprav. Rezultati raziskave podjetij Lookout (2011) in Juniper (2011), kažejo da se je v zadnjem obdobju močno povečala možnost okužba (malware, spyware) mobilne naprave pri prenosu

različnih programskih vsebin iz spleta. To predstavlja nekatere posredne grožnje mobilnim napravam, medtem ko poznamo tudi neposredne (odtujitev mobilne naprave, prestrezanje komunikacije, ipd). V vsakem primeru grožnje delujejo z namenom pridobitve nečesa, lahko so to podatki, naši avtentikacijski podatki (gesla, certifikati itd.) ali neposredni vstop v informacijski sistem organizacije, ki ga predstavljajo tudi podatki v oblaku.

3 PRI VPELJAVI RAČUNALNIŠTVA V OBLAKU JE SMOTRNO POZNATI

Spodnji model (Slika1) prikazuje enega od možnih načinov sistematičen vpeljave oblaka v organizacijo. V pri vrsti moramo znotraj organizacije (tudi znotraj že obstoječega informacijskega sistema) ugotoviti zakaj bomo storitev oblak uporabljali. Ali je to z namenom prenosa in hranjenja podatkov, uporabo aplikacij, ki nam jih ponudnik nudi ali oboje. S pomočjo teh informacij, lahko analizirano tudi procese in potrebe, ki so na procese vezane. Na podlagi teh informacij in informacij ki jih pridobimo z oceno informacijskega tveganja (informacije, programska oprema, itd..) lahko pričnemo z izborom tipa oblaka in možnih ponudnikov. V vseh segmentih takega izbora je zelo pomembno, da sodelujejo vse organizacijske strukture organizacije in seveda ključni kadri za informacijsko varnost.
S preudarnim in sistematičnim izborom oblaka, ki upošteva tudi zahteve informacijske varnosti, zmanjšamo verjetnost vpliva kombiniranih groženj na informacijski sistem organizacije.



Slika 1: Model izbora tipa oblaka

Pomembno je, da vsakokrat, ko implementiramo novo tehnologijo, kar računalništvo v oblaku zagotovo je, zastavimo temelje informacijske varnosti že v fazi načrtovanja sistema. Za optimalno asimilacije novosti je smotrno, da organizacija analizira svoje procese, jih po potrebi posodobi in usposobi svoje zaposlene. Vsak proces, ki se postavlja na novo ali se posodablja zaradi vpeljave računalništva v oblaku, je dobro preveriti skupaj z vsemi poglavitnimi udeleženci (predvsem pri prepletu z ostalimi organizacijskimi enotami). Le tako se dosežejo optimizacija, boljše in hitrejše prilagajanje in seveda višja stopnje varnosti.

4 MOŽNE REŠITVE

Najšibkejši elementi pri dostopanju do računalništva v oblaku s pomočjo mobilnih naprav, so uporabnik, njegova mobilna naprava in uporabnikovo pomanjkanje znanja o varni uporabi naprave. Uporabnike je treba informirati in izobraziti, kaj pomeni informacijska varnost pri rabi mobilne naprave, njene raznovrsten programske opreme in načinov povezovanja v oblak. Zavedati bi se morali tveganj in groženj, ki se jim izpostavljajo ob nevesti rabi informacijske tehnologije, Hkrati bi bilo treba poskrbeti za interne pravilnike, ki določajo ustrezno uporabo izročenih sredstev. S takim

pravilnikom organizacija definira vrsto mobilne naprave in programske opreme zanjo, ki ju je dovoljeno uporabljati, zaščitne metode in načine varnega povezovanja v oblak in prenašanja podatkov. Ugotovimo torej lahko, da je potrebno postaviti izhodišča za standardizacijo izročenih sredstev, ter s tem zagotoviti boljšo informacijsko varnost (Bernik in Prislan, 2010). Vsako nespoštovanje pravilnika se potem lahko sankcionira po vnaprej določenih pravilih organizacije.
Veliko je možnosti, kako lahko s pomočjo programskih nastavitev poskrbimo za varnost mobilne naprave. Pomembno je, da imamo na mobilni napravi nastavljena gesla za vstop v sistem in tudi za uporabo določenih funkcij. Dober primer so kode PIN pri pametnih telefonih. Pomembna je tudi enkripcija podatkov tako na sami napravi kot tudi pri prenosu podatkov. Se pravi, da je pomembno, da pri dostopanju do spleta in prenosu podatkov uporabljamo varnejšo povezavo, to je »https« povezavo. Avtentikacija s pomočjo certifikata pa zagotovi, da do določenih spletnih mest (lahko je to tudi dostop do podatkov v oblaku) ali mobilna banke dostopa samo ena mobilna naprava.

5 ZAKLJUČEK

Tehnološki napredek, tudi razvijajoče se področje računalništva v oblaku, je nemogoče zavreti. Napredne informacijske tehnologije prinašajo številne nove možnosti in prednosti, zato se niti posamezniki niti organizacije ne morejo več izogniti uporabi tehnoloških novosti. Tehnološke rešitve, ki bi pripomogle k celovitem zagotavljanju večjega nadzora mobilnih naprav in uporabnikovega početja (tudi povezovanja v oblak in prenosu podatkov) so trenutno še v fazi razvoja Istočasno pa je nesmiselno pričakovati, da bodo tehnološko varnostne rešitve v celoti rešile informacijsko varnostne probleme. Uporabniki so tisti, ki bodo morali paziti na pasti, ki jih ponuja novo tehnologija. Na vsakem posebej od njih je, da se dobro pouči o uporabi računalništva v oblaku, mobilni tehnologiji in varnostnih grožnjah ter vse možnosti uporablja varno, torej tako, da je tveganje čim manjše. Interni pravilniki, izobraževanja in vpeljava načel informacijske varnosti že ob načrtovanju novih procesov in organizacijskih struktur znotraj organizacije, bistveno povečajo informacijsko varnost. Organizacije pa bodo morale začeti ravnati bolj informacijsko varnostno osveščeno in se bolj dinamično prilagajati tehnološkim novostim. To pa je možno samo v primerih, da se potrebne segmente informacijske varnosti upošteva že pri izgradnji določenih delovnih okolij, procesov in organizacijskih struktur.

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. (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.

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.

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

Markelj, B., & Bernik, I. (2011). Kombinirane grožnje informacijski varnosti pri rabi mobilnih naprav. In *Nove razmere in priložnosti v informatiki kot posledica družbenih sprememb, 18. konferenca Dnevi slovenske informatike, Portorož, Slovenija, 18.-20. april 2011*. Ljubljana: Slovensko društvo Informatika.