Upravljanje varnostnih tveganj pri rabi mobilnih naprav

Igor Bernik, Fakulteta za varnostne vede, Univerza v Mariboru
Kaja Prislan, demonstratorka, Fakulteta za varnostne vede, Univerza v Mariboru

Namen in cilj prispevka
Upravljanje tveganj je pomemben proces identifikacije groženj in zavarovanja pred tveganji v informacijski varnosti. Prispevek prikazuje njihovo upravljanje in podaja glavne elemente v povezavi z rabo in dostopom do podatkov s pomočjo mobilnih naprav.

Metodologija
V prispevku so obdelana priporočila za upravljanje varnostnih tveganj. S pomočjo deskripcije so predstavljene ugotovitve, navedene so značilnosti upravljanja varovanja informacij, ki so posebne pri upravljanju tveganj v povezavi z mobilnimi napravami.

Ugotovitve in omejitve
Ugotovljamo, da so področja upravljanja informacijske varnosti in varnostnih tveganj ter rabe mobilnih naprav zelo povezani. V prispevku so prikazani krovni izsledki upravljanja varnostnih tveganj.

Izvirnost
Prispevek prikazuje povezavo med upravljanjem varnostnih tveganj in mobilnimi napravami. Izvirnost se kaže v tem, da je na omenjenem področju malo napisanega, da je v slovenskem prostoru upravljanje z informacijsko varnostjo v povezavi z mobilnimi napravami v povojih in da za to področje ne obstajajo ustrezna priporočila.

Ključne besede: upravljanje, tveganja, informacijska varnost, mobilne naprave

1 UVOD

Mobilne naprave (pametni telefoni, tablice, prenosni računalniki …) so postale pomemben del vsakdanjega življenja. So majhne, lahko prenosne, poleg tega pa imajo veliko računsko in spominsko zmogljivost. Žal te prednosti pomenijo tudi tveganja, saj jih je zaradi majhnosti lažje odtujiti, predvsem na javnih mestih, kot so letališki terminali, knjižnice in kavarne. Manjše in zmogljivejše ko so naprave, večje je število tatvin. Po navedbah NCIC[1] se je število prijavljenih kraj mobilnih naprav v ZDA od leta 2008 povečalo za 48 odstotkov v primerjavi s prejšnjima dvema letoma; s 73.700 na skoraj 109.000 (IEEE, 2009). V Sloveniji je po besedah odgovornih podobno, žal pa se tovrstni podatki ne zbirajo ločeno.
Uporaba mobilnih brezžičnih komunikacijskih naprav je porušila mejo med komunikacijo v informacijskem sistemu organizacije in zunanjim svetom. Dostop do pomembnih podatkov je zelo preprost in z vidika informacijske varnosti premalo zavarovan. Trenutno (še) ni preprostih in predvsem za uporabnike transparentnih rešitev, ki bi zaščitile mobilne naprave in komunikacijo s kibernetskim prostorom pred zlorabami. Mobilne naprave, uporaba katerih se stalno povečuje, nam omogočajo preprosto povezovanje v svet informacij. Dinamičen razvoj tehnologije, ozaveščenost, zahteve uporabnikov, hitre spremembe na pravem področju in kompleksnost sistemov zahtevajo ustrezno znanje. Zaradi kompleksnosti in neobvladljivosti informacijsko komunikacijskih tehnologij se stalno pojavlja potreba po zaščiti in zagotavljanju varnosti. Zagotavljanje varnosti pa se izvaja z izvajanjem ustreznih varnostnih mehanizmov, eden izmed njih je upravljanje varnostnih tveganj.
Osnovno poznavanje učinkovite in varne uporabe mobilnih naprav odpira mnogo varnostnih vprašanj, povezanih z dostopom do sistema. Z zmanjševanjem možnosti za nepooblaščen in/ali zlonameren vdor

[1] National Crime Information Center pod okriljem FBI.

v informacijski sistem, odtujitev in zlorabo informacij se krepi zaupanje v procese, transakcije in informacije, s katerimi se operira v določenem okolju. Zato je nujno vzpostavljanje in vzdrževanje varnega dostopa do informacij, shranjenih v informacijskem sistemu organizacije. Pri uporabnikih, ki mobilne naprave sočasno uporabljajo za poslovne namene (dostop do podatkov v centralnem informacijskem sistemu organizacije) in zasebno (igranje igric, uporaba spletnih aplikacij za dostop do banke, uporaba GPS-modula, itd), je večja verjetnost, da bodo tarča odtujitve podatkov ali druge grožnje, ki preti uporabnikom mobilnih naprav.
Iz tega sledi, da je informacijska varnost eden izmed najpomembnejših aspektov uspešnega delovanja vsake sodobne organizacije, saj ima v sodobnem času posamezna organizacija vizijo razvoja in delovanja podbrto z uporabo informacijskih sistemov in informacijsko komunikacijskih tehnologij. Za dosego strateškega cilja mora zagotoviti varno in nemoteno delovanje informacijskega sistema. Po mnenju Stoneburnerja, Gougena in Feringe (2002) je informacijsko področje najbolj izpostavljena in ob neprimerni zaščiti najbolj ranljiva točka organizacijske strukture. Organizacije morajo natančno poznati vsakršno grožnjo, ki preti njihovemu varnostnemu sistemu, sicer so posledice tveganja lahko usodne za njeno preživetje.

2 UPRAVLJANJE TVEGANJ

S pričetkom uporabe mobilnih naprav, smo odstranili mejo med internim informacijskim sistemom in zunanjim svetom. Informacijska varnost je ključni element integritete vsake organizacije, njenih zaposlenih, poslovnih procesov in informacij, ki jih uporablja pri delovanju. Tako poznavanje pravilne in varne uporabe mobilnih naprav in programskih dodatkov razumemo kot konkurenčno prednost v tekmi za prevlado v gospodarskem in znanstvenem svetu.
Da bi se zavarovali, je potreben nabor ukrepov, od defenzivnih do proaktivnih (Podbregar, 2008: 190). Pri načrtovanju ustrezne stopnje varnosti se moramo predvsem vprašati: »Če je neka informacija izgubljena, ali lahko škoduje organizaciji, oz. zagotovi prednost drugi« (Robinson, 1999)? Če je odgovor pritrdilen, je vzpostavitev varnostnih ukrepov za zavarovanje le-te neizogibna. S procesom upravljanja s tveganji se zagotavlja relativno varno in stabilno delovanje sistema, dostopa do podatkov in podatkov samih. Tveganja, ki jih pomenijo grožnje mobilni napravi, lahko škodujejo na ravneh:

- dostopa do občutljivih podatkov, shranjenih na napravi,
- dostopa do podatkov, shranjenih v korporativnem omrežju,
- zlonamerne programske opreme,
- sposobnosti nepooblaščenega izdajanja za pooblaščenega uporabnika.

Da zagotovimo varnost mobilne naprave, moramo poznati vsaj ključne varnostne grožnje v mobilnem svetu, ki so presenetljivo podobne kot grožnje v splošnem računalništvu. Zato potrebujemo podobno strategijo zaščite, kot jo uporabljamo za zaščito klasičnih računalnikov že dalj časa (Goodman in Harris, 2010). S tem zagotovimo vsaj osnovno zaščito pred morebitnimi zlorabami iz kibernetskega prostora in zmanjšamo izpostavljenost kibernetski kriminaliteti. Pri uporabnikovem povezovanju prek mobilne naprave je potrebna zaščita pred grožnjami pri dostopu do virov organizacije (NIST, 2009).
Vse dejavnosti, s katerimi se ukvarjamo, tudi nepomembne, spremlja določena stopnja tveganja, kar še posebej velja prav za uporabo mobilnih naprav. Tveganja so vseskozi prisotna tudi pri upravljanju in vodenju dejavnosti dostopa preko njih v informacijske sisteme organizacije. Ker ima vsaka organizacija svojo vizijo, ki jo zaradi narave sodobnega dela podpira z informacijsko tehnologijo, se tveganjem ne moremo izogniti niti na tem področju (Stoneburner, Goguen in Feringa, 2002). Pravzaprav je ravno nasprotno. Upravljanje s tveganji je eden najpomembnejših procesov, s katerim zagotavljamo relativno varno in stabilno delovanje organizacije, po mnenju Stoneburnerja idr. (2002) pa je kritičnega pomena tudi za izpolnjevanje zastavljene vizije.
Upravljanje s tveganji je tako proces, ki ga uporablja vodstvo, management in strokovno osebje za prepoznavanje ranljivosti pri rabi mobilnih naprav z namenom zagotavljanja zaupnosti, integritete in dostopnosti vseh komponent celovitega informacijskega sistema in naprav, ki se vanj povezujejo. Ker je organizacija odvisna od informacijske tehnologije, da bi se obdržala pri življenju in zagotovila poslovno uspešnost, morata informacijska varnost in disciplina upravljanja s tveganji postati integriran del organizacijske strukture (Whitman in Mattord, 2008: 297). Ker pa je uvedba in struktura sistema

odvisna od mnogih dejavnikov, kot so npr. finančne, kadrovske in materialne zmožnosti organizacije in volje njenega vodstva, je postopek upravljanja s tveganji odvisen od vsake organizacije posebej.
Ne glede na obliko takšnega sistema pa se vsak takšen proces začne z analizo tveganja in lahko temelji na različnih pristopih. Organizacija lahko izbira med štirimi različnimi pristopi (povzeto po Trček, 2006: 21-22) za upravljanje tveganj:

- Neformalen pristop: ne uporablja sistematičnih/strukturiranih metod. Njegova prednost je, da ne potrebujemo posebnega znanja in se lahko opravi v kratkem času. Slabost pa je možnost spregledanja nekaterih tveganj, rezultati so subjektivni, s čimer ni podlage za upravičenje vpeljevanja varnostnih mehanizmov.
- Splošen pristop; izbira standardiziranih varnostnih mehanizmov za vse dele informacijskega sistema in z njim povezane varnosti. Prednost se kaže v nepotrebnosti natančne analize, prav tako pa so izbrani varnostni mehanizmi uporabni na vseh organizacijskih področjih. Slabost se kaže v pretiravanju pri ugotavljanju varnostnih potreb.
- Natančna analiza; identifikacija in ocena premoženja, groženj in njihove resnosti skozi preučevanje ranljivosti tega premoženja. Prednost je vzpostavljanje ustrezne ravni/stopnje zaščite. Slabost pa široka potreba po kadrovskih, časovnih in finančnih virih.
- Kombinirana analiza; kritični deli/sistemi so podvrženi natančni analizi, medtem ko so ostali manj pomembni/ranljivi sistemi predmet osnovne analize.

Najbolj skrajen pristop pa je, kadar organizacija sploh ne upravlja s tveganji. Tovrstne organizacije naj resno razmislijo da si čimprej izberejo drugačen pristop, saj se jim v nasprotnem lahko zgodi, da ne bo več kaj obvladovati. Pri izbiri pravega pristopa, skladnega z organizacijsko strukturo, morajo nujno sodelovati in se povezovati različne osebe. Le-te lahko s svojim znanjem in izkušnjami pripomorejo k izbiri ustreznega pristopa, ki bo omogočil zagotovitev optimalne stopnje varnosti organizacije, glede na njeno strukturo in potrebe.
Pri vzpostavljanju sistema upravljanja s tveganji, organizacije lahko sledijo natančno določenim korakom, zaradi praktičnosti in racionalnosti pa jih navadno združujejo oz. preskočijo. Vsekakor je potrebno na začetku procesa identifikacije tveganj identificirati in oceniti lastno informacijsko premoženje, ki ga želimo zavarovati pred grožnjami. Naslednji korak v analizi tveganja je izračun tveganja oz. verjetnosti, da bo določena grožnja izkoristila določeno ranljivost. Možnost/verjetnost nezaželene posledice se kaže skozi tveganje, kar pomeni, da so tveganja in vplivi/učinki tesno povezani. Po izračunu verjetnosti, da bo grožnja uresničena, napravimo še izračun stroškov oz. posledic, ki bi pri tem nastale. Ta ugotovitev je ključnega pomena pri odločanju ali se bo določena šibka točka v informacijskem premoženju zavarovala. Posledice oz. stroški so torej osnova pri vpeljevanju varnostnih ukrepov.
Ranljivosti v informacijsko varnostnem sistemu so največkrat veliko večje kot vodstvo pričakuje, zato lahko realna ocena potencialne škode dvigne skrb in pripravljenost za vzpostavitev celovite in učinkovite informacijske varnosti na področjih, kjer je to najbolj potrebno (Pfleeger, 1989: 462).
Ob oceni vpliva in izračunu potencialnih stroškov[2] se mora organizacija odločiti, kaj je zanjo pomembnejše (Whitman in Mattord, 2008: 284-285):

- Stroški okrevanja zaradi uresničene grožnje in nastale posledice.
- Stroški zaščite pred grožnjami.

Posledice so lahko neposredne (uničenje ali poškodovanje premoženja) ali indirektne/posredne (izguba dobička ali ugleda). Posledica je lahko ocenjena s pomočjo dveh pristopov (Trček, 2006: 18):

- Ocena tveganja skozi kvalitativno merjenje učinkov/vpliva (uporabimo opisni kriterij).
- Ocena tveganja skozi kvantitativno merjenje učinka (npr. kolikšna bi bila finančna izguba).

Ocenjene stroške, ki bi nastali zaradi uresničene grožnje, nato uporabimo kot podlago za vpeljevanje nadzornih mehanizmov. Za vsako grožnjo in njej asociirano ranljivost, ki ima ostanek tveganja, ustvarimo pripravljalni seznam idej za nadzor (Whitman in Mattord, 2008: 286). Namen seznama, ki se začne z identifikacijo obstoječih kontrol, je torej identificirati območja ostankov tveganja. Ostanek tveganja je tisto tveganje, ki ostane kljub obstoječim kontrolam oz. nadzoru. Slednje je posledica organizacijskih, okoljskih, osebnih, tehnoloških in kulturnih ovir oz. omejitev (Trček, 2006: 19).

[2] Nekatere stroške je lahko določiti (npr. zamenjava strojne opreme), medtem ko so nekateri stroški zelo težko ocenjeni (npr. stroški nastali zaradi nepooblaščenega vstopa v informacijski sistem).

Ko se management organizacije odloči, da tveganja in grožnje informacijski varnosti ustvarjajo konkurenčno pomanjkljivost, pooblasti osebje, odgovorno za informacijsko tehnologijo in informacijsko varovanje za nadzor nad temi tveganji. Ko projektna skupina za razvoj informacijskega varovanja ustvari seznam ranljivosti, se mora odločiti za eno od štirih osnovnih strategij za nadzor tveganj, ki se pojavljajo iz naslednjega seznama (Whitman in Mattord, 2008: 297):

- Izogibanje: uporaba zaščite, ki izključi ali zmanjša preostala nenadzorovana tveganja.
- Prenos: premik tveganj na druga območja ali izven organizacijske entitete.
- Blaženje: zmanjšanje škode v primeru, da napadalec uspešno izkoristi ranljivost.
- Odobritev: razumevanje posledic in priznavanje tveganja brez poskusa nadzora ali blažitve.

Izbira prave strategije pa ni odvisna samo od identificiranih ranljivosti ter posledic, temveč je pogojena predvsem z možnostmi organizacije. Ali bo lahko določeno varnostno strategijo sploh vpeljala, je tako odvisno od njene organizacijske strukture, finančnih, kadrovskih, razvojnih in drugih zmožnosti.

Ko je strategija nadzora izbrana in uvedena, morajo biti kontrole redno nadzorovane in merjene, da bi ugotovili njihovo učinkovitost in ocenili preostanek tveganja, saj kljub nadzorovanim ranljivostim še vedno ostaja tveganje, ki ni bilo v celoti odstranjeno, premaknjeno ali planirano kot ostanek tveganj.

Čeprav se zdi nelogično, cilj informacijskega varovanja ni popolna odstranitev preostalih tveganj, saj absolutna varnost ni mogoča. Zato je temeljni cilj varnega informacijskega sistema, da so preostale grožnje na sprejemljivem nivoju tveganja, v skladu s potrebami organizacije. Če so bile osebe, ki odločajo, informirane o nenadzorovanih tveganjih in se primerne avtoritativne skupine, znotraj interesnih skupnosti, odločijo pustiti preostanek tveganja nenadzorovan, potem je program informacijskega varovanja izpolnil svoj cilj (Whitman in Mattord, 2008: 302-304).

Učinkovitost uvedenih kontrolnih mehanizmov merimo tako, da je le-ta enak stroškom uvedbe nadzorstva, zmanjšan za letne stroške varnostnih incidentov zaradi uvedbe nadzorstvenih mehanizmov. Končni rezultat je najboljši, kadar ugotovimo, da je bilo zmanjšanje tveganj večje kot stroški uvedbe nadzorstva (Pfleeger, 1989: 465). Da bi zagotovili čim večjo učinkovitost nadzornih mehanizmov, si lahko organizacije pomagajo z različnimi smernicami, priporočili in dobrimi praksami, ki omogočajo uvedbo takšnih nadzornih mehanizmov, ki se prilegajo konkretni organizacijski strukturi in ji zagotovijo tolikšno stopnjo varnosti, kot si jo same želijo.

3 ZAKLJUČEK

Zapisanih varnostnih omejitev in načinov obvladovanja tveganj se večina uporabnikov mobilnih naprav ne zaveda. Še huje, mnogi uporabniki niti ne uporabljajo varnostnih mehanizmov, ki jih mobilne naprave omogočajo brez dodatnih namestitev, le uporabiti jih je treba. Večina uporabnikov je prepričana, da je uporaba mobilne naprave vsaj toliko varna kot uporaba osebnega računalnika. Toda ni popolnoma tako, saj je mobilna naprava enako izpostavljena vdorom kot osebni računalnik, poleg tega pa je tveganjem izpostavljena še fizično in prek javnih mobilnih omrežij (GSM, UMTS, WiFi, itd), s tem pa so omogočeni še drugi načini napadov. Če poznamo grožnje, lahko ustrezno upravljamo s tveganji in zagotovimo varnejše delo in višjo varnost informacijskega sistema organizacije in naprave same.

Sklenemo lahko, da je stalen dostop v kibernetski prostor z mobilnimi napravami odprl mnogo priložnosti za napadalce in izpostavljenost uporabnikov za (kibernetsko) kriminaliteto, zato je upravljanje s tveganji nujno. Če se zavedamo, da omenjene naprave niso varne, in sprejmemo vsaj osnovne ukrepe za varnejše delo, pa se izpostavljenost tveganjem pomembno zmanjša. Izobraževanje in usposabljanje o nevarnostih mora na vseh ravneh družbenega življenja postati nekaj vsakdanjega, da usposobimo ozaveščenega posameznika, ki premišljeno in odgovorno uporablja mobilno napravo in varno uporablja stalen dostop v kibernetski prostor brez strahu pred zlorabo.

VIRI

Goodman, S., in Harris, A. (2010). Emerging Markets – The Coming African Tsunami of Information Insecurity. Communications of the ACM, 53 (12), str. 24–27.

IEEE, 2009: http://www.ieee-infocom.org/2009/demos/4%20-%20A%20pervasive%20mobile%20device%20protection%20system.pdf (pridobljeno 4. 5. 2010).
NIST, 2009: http://csrc.nist.gov/news_events/HIPAA-May2009_workshop/presentations/7-051909-new-technologies-mobile-devices.pdf (pridobljeno 22. 11. 2011)
Pfleeger, C.P. (1989). Security in Computing. Englewood Cliffs: Prentice-Hall.
Podbregar, I. (2008). Vohunska dejavnost in gospodarstvo. Ljubljana: Fakulteta za varnostne vede.
Robinson, R.R. (1999). Issues in security management; thinking criticaly about security. Woburn: Butterworth. Heinemann.
Stoneburner, G., Goguen, A. in Feringa, A. (2002). Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology. Pridobljeno 25.11.2009, s http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
Trček, D. (2006). Managing Infomation Systems Security and Privacy. Berlin: Springer.
Whitman, M.E in Mattord, H.J. (2008). Management of Information Security. Boston: Course Technology Cengage Learning.