Uporaba ISO-standardov skozi informacijsko varnostne politike nadzora dostopa do informacijskega sistema

Denis Zver, Igor Bernik

Namen prispevka
Varovanje podatkov in informacij v podjetjih predstavlja pomemben dejavnik pri delovanju v poslovnem svetu. Varnostne politike so temelj vsakega varnostnega načrta. Definirajo pravila, cilje in odgovornost pri delu v informacijskih sistemih podjetja. Ker so med podjetji razlike oziroma specifike v načinu delovanja, univerzalna varnostna politika ne obstaja, ampak si podjetja pri njenem ustvarjanju lahko pomagajo z različnimi standardi, kot so na primer ISO-standardi, ki dajejo smernice in priporočila, kako zagotoviti varnost informacijskega sistema. Na voljo je več standardov, zato smo se v prispevku osredotočili na serijo standardov ISO/IEC 27000, natančneje ISO/IEC 27002.

Metodologija
V prispevku je uporabljena deskriptivna metoda s pregledovanjem različnih primarnih in sekundarnih virov. Uporabljena je tudi primerjalna metoda, na podlagi katere smo prišli do zaključnih sklepov.

Ugotovitve
Dokumenti varnostne politike igrajo pri zagotavljanju varnosti informacijskih sistemov pomembno vlogo. Pomemben del ustvarjanja varnostne politike so tudi ISO-standardi, ki podjetjem pomagajo ustrezno zaščititi svoje informacijske sisteme pred nepooblaščenimi vdori in drugimi grožnjami. Standard ISO/IEC 27002 je specializiran tudi za področje nadzora dostopa do informacijskih sistemov, zato je pri pripravljavcem politike nadzora dostopa lahko v veliko pomoč.

Izvirnost/pomembnost prispevka
Izvirnost in pomembnost prispevka se kaže v osvetlitvi problematike uporabe ISO-standardov za ustvarjanje ustrezne varnostne politike predvsem za nadzor oziroma obvladovanje dostopa do informacijskih sistemov.

Ključne besede: ISO-standardi, informacijski sistem, nadzor dostopa, varnostna politika

1 Uvod

Strokovnjaki za informacijsko varnost posameznike, podjetja, javne ustanove in druge organizacije opozarjajo na previdnost pri uporabi informacijskih sistemov, le-ti še vedno podcenjujejo nevarnosti nezadostne ali neustrezne zaščite sistemov. Zagotavljanju informacijske varnosti ni namenjene dovolj pozornosti, še manj finančnih sredstev. Ker so podatki v osrčju organizacije pogosto njena najpomembnejša dobrina, jih je posledično potrebno ustrezno zaščititi. Neustrezno upravljanje s podatki jih izpostavlja in omogoča dostop do njih nepooblaščenim osebam, kar pa lahko vodi v zlorabo podatkov ali nesrečo. Podjetja morajo upoštevati možnost morebitnih zlonamernih dejanj posameznikov ali organiziranih skupin zunaj ali znotraj podjetja.

Z izpostavljanjem ali izgubo podatkov podjetja tvegajo motnje v utečenih poslovnih procesih, izgubo konkurenčne prednosti, škodljiv vpliv za dobro ime podjetja, finančno škodo in kaznovalne ukrepe vladnih ali industrijskih organizacij zaradi posledične neskladnosti z zakoni ali standardi in predpisi (Realsecurity, 2008). Z namenom, da se zagotovijo ustrezni mehanizmi zaščite informacijskih sistemov, obstajajo splošni kodeksi najboljših praks in priporočil za zagotavljanje informacijske varnosti, med katerimi je najbolj znana in široko sprejeta serija standardov je ISO/IEC 27000. Le-ta opredeljuje večino proceduralnih, organizacijskih, fizičnih in drugih problemov, ki se nanašajo na zagotavljanje informacijske varnosti. Serija standardov ISO/IEC 27000 deluje na principu proaktivnega pristopa in uporabi najboljših praks z namenom uveljavitve varnega in neprekinjenega poslovanja ter zagotavljanja ciljnega nivoja varnosti. Omenimo še smernice The Best Practise in Information Security, organizacije ISF (Information Security Forum, 2012), ki predlagajo primerljive ukrepe kot standardi serije ISO/IEC 27000, pri čemer posamezna področja varnosti globje razdelajo. Obdelana pa so tudi področja, ki jih standard ISO/IEC 27002 izpusti, kot npr. napadi kibernetskih kriminalcev, računalništvo v oblaku, virtualizacija, kritična infrastruktura in drugi.
Namen standardov informacijske varnosti je, da so načrtovalcem, razvijalcem, uporabnikom in vzdrževalcem v pomoč pri usmerjanju rabe informacijskih sistemov. Ker so napadalci aktivni pri pridobivanju znanja in veščin, ter se stalno poslužujejo novih načinov in tehnik za nelegalen dostop do informacijskih sistemov, je pomembno, da so v podjetjih postavljeni visoki standardi (informacijske) varnosti in kakovostne, predvsem pa učinkovite varnostne politike.

2 Standardizacija

Inštitut za standardizacijo (2008) le-to definira kot dejavnost vzpostavljanja usklajenih pravil in določil za ponavljajočo se uporabo, da se doseže optimalna stopnja urejenosti na nekem področju. Standardi so sporazumi, osnovani na priznanih rezultatih znanosti, tehnike in izkušenj, pripravljeni z namenom doseganja optimalnega, predvsem pa varnega delovanja podjetij. Standardizacija je način, kako spodbuditi uporabo najboljših praks in zahtev za zagotovitev transparentnosti produktov in storitev na svetovnem trgu. Istočasno pa je to tudi način kako potrditi skladnost mehanizmov za preverjanje, ali ti produkti in storitve dosegajo nivoje standardov Mednarodne organizacije za standardizacijo (ISO, 2008).
Standardi informacijskih sistemov po Tsohou, Kokolakis, Lambrinoudakis in Gritzalis (2010) prinašajo več prednosti:

- ustvarjajo konsenz glede terminologije,
- ustvarjajo skupno razumevanje in soglasje glede funkcionalnih in nefunkcionalnih zahtev pri načrtovanju sistemov, ki zagotavljajo združljivost opreme različnega porekla,
- krepijo interoperativnost.

Te se nanašajo tudi na varnost informacijskih sistemov, saj standardi spodbujajo skupno razumevanje varnostnih zahtev in zagotavljajo da so implementirani mehanizmi v skladu z globalno sprejetimi pravili in prakso. Na ta način informacijski sistemi dosegajo splošno sprejete nivoje varnosti ter učinkovito in varno delujejo tudi v povezavi z drugimi sistemi.
Obstaja večje število organizacij za standardizacijo, ki jih glede na njihov obseg delovanja lahko razdelimo na mednarodne, regionalne in nacionalne. Organizacije, ki so izdale standarde za informacijsko varnost in dosegle večjo sprejetost vključujejo ISO, Information Systems Audit and Control Association (ISACA), Information Systems Security Association (ISSA), National Institute of Standards and Tehnology (NIST), British Standards Instituition (BSI), Information Security Forum (ISF), Payment Card Industry Security Standards Council (PCI-SSC) in druge. Nekateri varnostni

standardi se stalno posodabljajo in čedalje bolj uveljavljajo, drugi podajajo smernice, primere dobre prakse, le nekateri izmed njih pa omogočajo končno certifikacijo (Tsohou et al., 2010).
Kljub širokem naboru standardov, ki pokrivajo splošna in specifična področja informacijske varnosti, pa poznavanje sprejetih in uveljavljenih standardov ostaja dokaj majhna. Raziskave vdorov v informacijske sisteme (Tsohou et al., 2010) v Veliki Britaniji kažejo, da se samo 21 odstotkov podjetij zaveda obstoja standarda ISO serije 27000, le 30 odstotkov teh podjetij pa ima navedene standarde implementirane, podobno pa ugotavljata tudi Bernik in Prislan (2011) za slovenska podjetja, saj le 55 odstotkov pozna ISO/IEC 27000 serijo standardov, le 11 odstotkov med njimi pa ima standard implementiran.

2.1 Varnostne politike in nadzor dostopa

Varnostna politika organizacije je skupek pravil, napotkov in postopkov, ki opredeljujejo, kako v organizaciji upravljati, ščititi in ravnati z določenimi resursi z namenom doseganja konkretno zastavljenih varnostnih ciljev (Belič in Lesjak, 2006). Zagotavljati mora smernice za varnost informacijskega sistema podjetja in zajemati področja, kot so uporaba interneta in notranja uporaba omrežja, zasebnost podatkov, odzivanje na varnostne incidente, varnost dokumentov, vprašanja človeških virov in drugo. Je oblika pisnega sporazuma o pogojih in pravilih varnega dela, ki mora biti prebran in podpisan s strani zaposlenih. Uporaba politike pomaga izobraževati zaposlene o vrstah orodij, ki jih bodo uporabljali v informacijskem sistemu in kaj lahko od teh orodij pričakujejo. Politika naj prav tako opredeljuje meje obnašanja oziroma vedenja pri delu z informacijskimi sistemi in določa posledice kršitev. Uporaba varnostne politike za varovanje informacijskih sistemov v podjetju je pomembna za zagotavljanje celovite organizacijske varnosti in tudi za lažje postopanje glede pravne odgovornosti v primeru varnostnih incidentov. Gerber in Solms (2008) navajata, da se podjetja pri svojem delu srečujejo z vedno več različnimi kompleksnimi varnostnimi zahtevami, poleg tega pa jih pri tem omejujejo še mnoge zakonske ureditve. Veliko različnih zakonov, pravilnikov in standardov v različnih regijah vse to še otežuje. Vedno bolj se poudarja tudi dejstvo, da vlaganje v informacijsko varnost ne predstavlja samo naložbe, ampak je to bistvenega pomena za preživetje podjetja, v nekaterih primerih pa celo ustvarjanje konkurenčne prednosti.
Za nadzor dostopa do informacijskega sistema se smiselno uporabljata standarda ISO/IEC 27002 – standard dobrih praks za zagotavljanje varnosti informacijskega sistema v skladu s standardom ISO/IEC 27001. Definira postopke za zmanjšanje tveganja in obvladovanje pomanjkljivosti sistema. Podjetja lahko v praksi uporabijo dodatne postopke, ki so najprimernejši za določeno organizacijsko okolje (Ratchakom, Prompoon, 2011). Omenjeni standard opredeljuje 133 varnostnih kontrol, razdeljenih med 11 vsebinskih področij. Vsebinska področja si sledijo v naslednjem vrstnem redu (ISO/IEC 27002, 2012): varnostna politika, organizacija varovanja informacij, upravljanje sredstev, varovanje človeških virov, fizična zaščita in zaščita okolja, upravljanje s komunikacijami in s produkcijo, nadzor dostopa, nakup, razvoj in vzdrževanje informacijskih sistemov, upravljanje incidentov pri varovanju informacij, upravljanje neprekinjenega poslovanja, združljivost.
Da bi podjetja identificirala in izbrala primerne varnostne kontrole, je treba jasno opredeliti varnostne zahteve za zagotovitev varnosti informacijskih sistemov v kontekstu svojega poslovanja oziroma potrebam poslovnega okolja, v katerem delujejo. Pri uporabi standarda je potrebno uporabiti strukturirani pristop, ki je osnovan na specifičnosti varnostnih zahtev organizacije (ISO/IEC 27002, 2012). Po standardu ISO/IEC 27002 (Gerber et. al., 2008) je za oceno in izbiro ustreznih mehanizmov za zagotovitev informacijske varnosti potrebno pridobiti informacije s treh področij oziroma virov, in sicer:

- ocenitev varnostnih tveganj; identificiranje ranljivosti, groženj in verjetnosti, da pride do izpostavitve teh ranljivosti ter možnih posledic;
- procesiranje informacij na edinstven način; organizacije delujejo na specifičen način z različnimi cilji, razvijajo lastne načine procesiranja informacij, ki podpirajo njihovo obliko poslovanja;
- skladnost s pravnimi predpisi; predstavljene so zakonske omejitve, skladnost s predpisi, statuti in drugimi oblikami pogodbenih razmerij, ki vežejo podjetje z njegovimi poslovnimi partnerji, ponudniki storitev in dobavitelji; standard ne predpisuje, da mora organizacija uvesti vsa priporočila, ki so omenjena, ampak se ta odloča na podlagi tveganj, ki nastopajo v organizaciji.

Nadzor dostopa oziroma obvladovanje dostopa pojasnjuje Hajtnik (2002) kot nadzor dostopa do informacijskih sistemov in podatkov ter njihovo uporabo. Navaja, da se obvladovanje dostopa nanaša na obvladovanje fizičnega dostopa (npr. ključi, kartice itd.) in na obvladovanje programske opreme (npr. kako preprečiti nepooblaščeni dostop do sistemov informacijske tehnologije in podatkov). Za to so potrebne razne oblike kontrol, razni načini upravljanja z uporabniškimi dostopi, gesli, pravicami dostopa, posebnimi pravicami, omejevanje storitev. Dostop do informacijskih sistemov, omrežij in podatkov mora biti za preprečevanje neavtoriziranega dostopanja primerno nadzorovan. Nadzor dostopa je v ISO/IEC 27002:2005 (ISO/IEC 27002, 2012) opisan v enajstem tematskem poglavju in zajema naslednje vsebine:

- poslovne zahteve pri nadzoru dostopa;
- upravljanje dostopa uporabnikov; odgovornosti uporabnikov;
- nadzor dostopa do omrežja;
- nadzor dostopa do operacijskega sistema;
- nadzor dostopa do aplikacij in informacij;
- mobilno računalništvo in delo na daljavo.

Zahteve podjetja glede nadzora dostopa do informacijskih sistemov morajo biti jasno dokumentirane v politiki nadzora dostopa: Ta mora vključevati profile za dostop glede na vrsto dela (role based access control). Dodeljevanje pravic za dostopanje uporabnikom mora biti formalno nadzorovano preko registracije uporabnikov in administrativnih postopkov (od prve registracije uporabnika do odstranitve pravice dostopanja, ko le-ta ni več potrebna). Vključujejo posebne omejitve pri dodeljevanju pooblastil in upravljanju z gesli ter izdajanje rednih poročil o pravicah za dostopanje. Uporabnike je treba podučiti o njihovih obveznostih vzdrževanja učinkovitega nadzora dostopa (npr. uporaba ustreznih gesel in ohranjanje njihove tajnosti). Sistemi in informacije morajo biti zavarovane v primerih, ko uporabnik zapusti prostor (pospravi mizo in zaklene namizje). Nadzorovati je potrebno tudi dostop do omrežnih storitev znotraj organizacije in širše.
V skladu z zahtevo standarda ISO/IEC 27002 (2012) je potrebno ustrezno definirati varnostno politiko in zagotoviti primerno overjanje uporabnikov, ki dostopajo iz oddaljenih lokacij. Problematično je predvsem zunanje oziroma oddaljeno dostopanje. V teh primerih je nujno zagotoviti močnejše metode overjanja, npr. kriptografsko overjanje. V primerih, da organizacije operirajo z večjimi informacijskimi sistemi, je priporočljiva segregacija sistema na ločene domene; na primer javno dostopne sisteme, interna omrežja in kritične sisteme. Dostopanje do aplikacij sistemov mora biti nadzorovano v skladu z definirano politiko nadzora dostopa. Občutljivejšim aplikacijam je treba zagotoviti izolirane platforme in/ali dodatne nadzorne funkcije, če delujejo na skupnih platformah. Pri upravljanju mobilnega računalništva in oddaljenega dostopanja je potrebno zapisati formalne politike, ki pokrivajo varno uporabo prenosnih računalnikov,

dlančnikov, mobilnih telefonov in podobnih naprav ter varno delo na daljavo (delo od doma in druge oblike dela na daljavo).

Na podlagi opisanih vsebin standarda ISO 27002 ugotavljamo, da standard v priporočilih za nadzor dostopa zajema široko paleto različnih situacij in ukrepov, kako zagotoviti ustrezno stopnjo varnosti informacijskega sistema sodobnega podjetja ali kakršnekoli organizacije, ki dela z informacijskimi viri. Standard se osredotoča na zagotavljanje varnosti na več področjih (ISO/IEC 27002, 2012):

- Dobra varnostna politika – proceduralni vidik varovanja informacijskega sistema. Ta vidik je poudarjen pri vsakem specifičnem področju nadzora dostopa, saj predstavlja osnovo, na podlagi katere so zastavljeni vsi ukrepi in varovalke.
- Tehnične kontrole – različne oblike uporabniških vmesnikov. Sem sodijo dodeljevanje gesel, pooblastil, spremljanje uporabe dostopa in drugo.
- Fizične oblike nadzora – nadzor delovnih postaj zaposlenih ter različnih pripomočkov in orodij, ki jih uporabljajo (prenosni računalniki, mobilni telefoni, tiskalniki, fotokopirni stoji, …). Poleg tega, da se s fizičnimi kontrolami dostopa preprečuje izguba podatkov, je ta namenjena tudi zaščiti v primerih naravnih nesreč, kot so požari, poplave in podobni dogodki.

Podjetja se za uporabo predlaganih mehanizmov zaščite odločijo na podlagi lastnih potreb oziroma specifike okolja, v katerem delujejo. Ni nujno, da vzpostavijo vse predlagane mehanizme standarda ISO 27002, ampak se lahko odločijo za tiste, ki jim omogočajo doseganje želene stopnje varnosti in zagotavljanje nemotenega delovanja.

3 Zaključek

Preko priporočil, ki temeljijo na standardu ISO/IEC 27002 so predstavljeni temeljni pojmi standardizacije in snovanja varnostnih politik za nadzor dostopa do informacijskih sistemov. Poleg omenjenega standarda področje varovanja informacij pokriva večje število standardov, vendar je opisani v poslovnih okoljih razvitega sveta med bolj uporabljanimi. Standardi predstavljajo osnovo za izdelavo varnostnih politik v podjetjih, le ta pa se morajo zavedati, da povečevanje odvisnosti od informacijske tehnologije prinaša mnoge nevarnosti in tveganja, zato je nujno potrebno, da se ustrezno pripravijo na tovrstne izzive in predvsem povečajo preventivno delovanje (Bernik in Prislan, 2011). Mnogo podjetij se omenjenih nevarnosti ne zaveda, posledično se jim vlaganje sredstev za ustrezne varnostne mehanizme ne zdi smiselno. Ker se delovno okolje in kibernetski prostor stalno razvija, je potrebno tudi varnostno politiko stalno posodabljati. Ker ni mogoče predvideti vseh možnih situacij, mora sprejemljiva uporaba varnostne politike obravnavati tudi možnost, da pride do dogodka, ki v varnostni politiki ni predviden. Če zaposleni upoštevajo pravila sprejete varnostne politike, bo njihova izpostavljenost varnostnim incidentom manjša, hkrati pa varnostna politika zaposlene zaščiti pred nevarnimi poskusi napadalcev, ki npr. z uporabo tehnik socialnega inženiringa in drugimi metodami poskušajo nelegalno dostopati do informacijskih sistemov in tajnih podatkov in jih v primeru sledenja dokumentiranih postopkov odvezuje njihove odgovornosti.

Pripravljavci politike so razpeti med željami in potrebami po ureditvi celotnega področja informacijske varnosti ter hitrim reševanjem perečih problemov. Glede na vedno bolj omejene vire in sredstva se je smiselno posvetiti tistim področjem, ki so najbolj kritična z vidika zagotavljanja neprekinjenega poslovanja in izpostavljenosti tveganjem. Eno izmed teh področij je vsekakor nadzor dostopa do informacijskega sistema, pri čemer nam standard ISO/IEC 27002 lahko precej pomaga. Pri tem ne smemo pozabiti, da je izdelava informacijske varnostne politike

zahteven in dolgotrajen proces, ki je ključnega pomena za zagotavljanje ustrezne varnosti podatkov (Milanič, 2009).

Informacijske varnostne politike so za zagotavljanje ustrezne stopnje informacijske varnosti, glede na znane faktorje tveganja smiselne in povečini potrebne, saj jasno opredeljujejo odgovornosti zaposlenih in princip delovanja nadzora dostopa do in pretoka informacij. Ustrezna predstavitev, uvajanje in razumevanje zagotavlja, da imajo zaposleni jasne smernice operiranja s podatki. To pa skupaj z visoko stopnjo organizacijske kulture (ki jo zagotavljajo tudi uvedeni postopki) zagotavlja ustrezno stopnjo zaščite informacijskega sistema in informacijske varnost.

4 Viri in literatura

Bernik, I., Prislan, K. (2011). Information Security In Risk Management Systems: Slovenian perspective. *Varstvoslovje*, 13 (2), 208-221.

Gerber, M. in Solms, R. (2008). Information security requirements – Interpreting the legal aspects. *Computers & Security*, 27, 124 - 135.

Hajtnik, T. (2002). *Priporočila za pripravo informacijske varnostne politike.* Ljubljana, Center Vlade RS za informatiko.

Information Security Forum, (2012). *Standard of Good Practice for Information Security*. Pridobljeno 16. 6. 2012 na: www.securityforum.org/?page=2011sogppublicorder

Inštitut za standardizacijo. (2008). *Sistem standardizacije v Sloveniji*. Pridobljeno 18.4.2010 na: http://www.sist.si/index.php?option=com_content&view=article&id=76&Itemid=108&lang=sl

ISO, (2008). *ISO in brief*. Pridobljeno 18.4.2010 na: http://www.iso.org/iso/isoinbrief_2011.pdf

ISO/IEC 27002, (2012). *ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management*. Pridobljeno 18.4.2012 na: http://www.iso27001security.com/html/27002.html#Section2

Milanič, E (2009). *Odločitveni model za podporo pri izdelavi informacijske varnostne politike*. Magistrsko delo, Kranj, Univerza v Mariboru, Fakulteta za organizacijske vede.

Ratchakom, M. in Prompoon, N., (2011). A process model design and tool support for information assets access control using security patterns. *Computer Science and Software Engineering (JCSSE)*, 307-312.

Realsecurity, (2008). Kriptografija – Zaščita podatkov in procesov. *Realsecurity Info – Specializirana revija za elektronsko varnost,* 6, 5 – 8.

Tsohou, A., Kokolakis, S., Lambrinoudakis, C. in Gritzalis, S. (2010). A security standards' framework to facilitate best practices' awareness and conformity. *Information Management & Computer Security*, 18, 350 – 365.