Varnostna politika informacijskega sistema

Robert Kralj, študent, Fakulteta za varnostne vede, Univerza v Mariboru

Namen prispevka
Namen prispevka je opredeliti varnostno politiko kot ključni branik varovanja informacij v organizaciji pred različnimi zunanjimi in notranjimi vplivi, ki bi lahko posegli v celovitost informacijskega sistema in s tem organizacije kot celote. Celovita varnostna politika zagotavlja stabilnost informacijskega sistema, zaupnost, transparentnost, varuje informacije in vitalne poslovne procese, ki so nujni za uspešno delovanje podjetja. V prispevku sem opredelil varnostno politiko in njen pomen v podjetjih, ter navedel najpomembnejše elemente za pripravo učinkovite varnostne politike.

Metodologija
Uporabil sem teoretično deskriptivno metodo s študijem, uporabo in interpretacijo slovenske in tuje literature. Osnovo predstavlja lastno teoretično in praktično znanje.

Ugotovitve
Varnostne grožnje s katerimi se soočajo podjetja so realne in še naraščajo.
Kvalitetno varnostno politiko zagotavlja skladnost le-te z mednarodnimi standardi ISO 17799:2000 (ISO 27002:2005), in ISO 27001:2005. Podjetja se soočajo z različnimi varnostnimi incidenti vsaj enkrat letno, kar povzroča motnje v poslovanju, izgubi strank, poslovno škodo. Učinkovita varnostna politika je nujna za stabilnost in uspešnost podjetja.

Praktična uporabnost
Okrepiti zavedanje o pomenu varnostne politike za stabilnost in uspešnost podjetja, sploh glede na dejstvo da veliko slovenskih podjetij temu področju ne posveča dovolj, ali sploh nobene pozornosti.

Izvirnost/pomembnost prispevka
V prispevku je navedena definicija varnostne politike informacijskega sistema. Navedeni so ključni elementi za sestavo učinkovite varnostne politike na strateški ravni. Prispevek je namenjen vodstvenim kadrom podjetij in organizacij, ki se soočajo z varnostnimi grožnjami in incidenti ter posledično želijo/potrebujejo varnostno politiko.

Ključne besede: informacijski sistem, varnostna politika, informacije, poslovni procesi, varovanje podatkov, varnostne grožnje

1 UVOD

Varnostna politika predstavlja ključni branik varovanja informacij v organizaciji pred različnimi zunanjimi in notranjimi vplivi, ki bi lahko posegli v celovitost informacijskega sistema in s tem organizacije kot celote. Celovita varnostna politika zagotavlja stabilnost informacijskega sistema, zaupnost, transparentnost, varuje informacije in vitalne poslovne procese, ki so nujni za uspešno delovanje podjetja. V članku bom opredelil varnostno politiko in njen pomen v podjetjih, ter navedel najpomembnejše elemente za pripravo učinkovite varnostne politike.

2 OPREDELITEV VARNOSTNE POLITIKE

Štrakl (2003) definira varnostno politiko informacijskega sistema kot celovit pogled na varnost informacijskega sistema in zajema vse dejavnike, organizacijska pravila in postopke, ki kakorkoli vplivajo na varno in zanesljivo delovanje celotnega informacijskega sistema.

Varnostna politika predstavlja osnovni temelj, na katerem lahko razvijemo učinkovit in celovit program varnosti. Varnostna politika pomeni tudi implementacijo varnostnih pričakovanj managerjev v praksi, v obliki specifičnih, izmerljivih in preverljivih ciljev ter nalog (Weise in Martin, 2001).
Informacijska varnostna politika je načrt, ki opisuje cilje postopkov. Varnostna politika ni smernica ali standard, niti ni postopek, pač pa načrt za celovit program varnosti. Varnostna politika definira varnost tako kot specifikacija nekega izdelka definira izdelek (Barman, 2002).
Varnostno politiko lahko opredelim kot celovit načrt varovanja informacij in delovnih procesov v organizaciji, ki je kot tak zavezujoč za vse zaposlene, pred različnimi (neželenimi) zunanjimi in notranjimi vplivi, ki ogrožajo informacijsko varnost neke organizacije in varnost organizacije kot celote.

2.1 Pomen varnostne politike

Osnovni namen varnostne politike je obveščanje uporabnikov, zaposlenih, in managerjev o bistvenih zahtevah, ki morajo biti izpolnjene za učinkovito varovanje ljudi, strojne in programske opreme in informacij (Weise in Martin, 2001). Varnostna politika torej mora opredeliti tiste mehanizme, preko katerih bo možno zagotovo ustrezen sistem varovanja. Informacijska varnostna politika zato postavlja osnovo, na kateri se zgradi varen računalniški sistem in omrežje v podjetju.
Raziskava ISBS[1] o informacijski varnosti iz leta 2010, ki jo je izvedlo podjetje Price Waterhouse Coopers in je zajela preko 500 malih, srednjih in velikih podjetij kaže, da je varnostna politika v podjetju nujen element. Kaj je raziskava pokazala? :

- 92% velikih podjetij se je v zadnjem letu soočilo z vsaj enim varnostnim incidentom,
- 45 poskusov zaobiti varnostne mehanizme v povprečju v vsakem velikem podjetju,
- 83% malih podjetij je imelo vsaj en varnostni incident v preteklem letu,
- 14 poskusov zaobiti varnostne mehanizme v povprečju v vsakem malem podjetju,
- 62% velikih podjetij je bilo okuženih z virusom ali zlonamerno programsko opremo v preteklem letu,
- 61% velikih podjetij je zabeležilo poskus vdora v njihovo omrežje,
- 15% velikih podjetij je zabeležilo dejanski nepooblaščen dostop v njihovo omrežje,
- 25% velikih podjetij je zabeležilo DO^{2}S napad oz. onemogočanje storitve v preteklem letu.
- Zanimivi so tudi rezultati o odzivih podjetij na varnostne grožnje:
- 77% zaposlenih je prepričanih, da njihov management posveti veliko pozornosti informacijski varnosti,
- Mala podjetja namenijo v povprečju približno 10% svojega IT budgeta za svojo varnost,
- 90% velikih podjetij ima dokumentirano varnostno politiko,
- 68% velikih podjetij ima implementirano varnost politiko po standardu ISO 27001,

Kot lahko vidimo se podjetja soočajo z realnimi varnostnimi grožnjami. Ker pa številke o napadih same o po sebi ne povedo veliko, je potrebno navesti še dejanske posledice tovrstnih napadov in groženj. Ločimo več vrst posledic varnostnih incidentov:

- finančne posledice,
- posledice ki se nanašajo na ugled in dobro ime podjetja,
- motnje in onemogočanje poslovanja,
- preiskave incidentov terjajo veliko časa in denarja,
- težave s povrnitvijo v prejšnje stanje,
- izguba strank in dohodka,
- nestabilnost podjetja,
- v nekaterih primerih tudi propad podjetja.

Zapisano kaže, da je učinkovita varnostna politika v času ko si uspešnega poslovanja brez informacijske tehnologije ne gre več zamisliti, nujna za dolgoročen obstoj podjetja. Na to kažejo tudi finančne posledice varnostnih groženj. Po podatkih ISBS (2010), je 2-4 dnevni izpad poslovanja

[1] ISBS-Information Security Breaches Survey 2010.
[2] DOS-Denial of service oz. onemogočanje storitve.

zaradi neustrezne varnosti v malem podjetju povzročil 15,000-30,000 funtov škode, v velikih podjetjih pa je 2-5 dnevni izpad v povprečju povzročil 200,000-380,000 funtov škode. Največji varnostni incident je mala podjetja v povprečju osiromašil za 3,000-5,000 funtov, velika pa med 25,000 in 40,000 funtov. Ob tem ni upoštevanih še posrednih stroškov, kot je recimo izguba intelektualne lastnine. Tako je eno izmed velikih glasbenih podjetij v raziskavi zaradi varnostne luknje v sistemu izgubilo več kot 100,000 funtov, saj je album znanega glasbenika »pobegnil« v javnost še pred predvideno izdajo. To je za seboj potegnilo celo vrsto posledic, od izgube neposrednega dohodka od prodaje, do izgube ugleda in zanesljivosti, medijske nezainteresiranosti etc.
Celovita varnostna politika v podjetju zavaruje informacije in informacijski sistem, varuje poslovne procese, pripomore k ugledu in dobremu imenu podjetja, preprečuje oz. omejuje poslovno škodo, omejuje motnje in onemogočanje poslovanja, olajša delovne procese in delo zaposlenih, omejuje in preprečuje dolgoročne neželene posledice morebitnih varnostnih incidentov, zagotavlja stabilnost podjetja ter obstoj podjetja na dolgi rok.

3 MEDNARODNI STANDARDI

Temelj informacijske varnosti predstavlja standard ISO 1779:2000. Standard ISO 17799 je zbirka pravil in metod nadzora za področje informacijske varnosti (Frešer 2009).
Je mednarodno veljaven standard, namenjen vodstvenemu osebju, ter predstavlja model za učinkovit sistem upravljanja varovanja informacij (SUVI). Sestavljen je iz dveh delov. Prvi del predstavlja najboljšo prakso pri zadovoljevanju zahtev standarda in razlaga, kaj naj bi organizacija imela. Drugi del je specifikacija z napotki za uporabo in razlaga, kaj organizacija mora imeti, če želimo biti skladni s standardom in se po njem certificirati (Ključevšek, 2002). Pomembno je opomniti, da so standard ISO 17799 v letu 2007 preimenovali v standard ISO 27002:2005, vendar ni bilo nikakršnih vsebinskih ali oblikovnih sprememb. Tako so ga imensko zbližali z drugim sorodnim standardom, ISO 27001:2005.

Standard ISO 27001 je nekoliko manj obsežen. Kosutic (2010) pravi, da se ISO 27001 bolj osredotoča na vlogo managementa pri informacijski varnosti. Po njegovem mnenju, se ISO 27001 uporablja za postavitev temelja oz. okvira informacijske varnosti v podjetju, medtem ko ISO 27002 določa konkretno implementacijo nadzora in kontrole. Avtor nadaljuje da združitev standardov ne bi predstavljala ustrezne rešitve, saj bi dobili en sam preobsežen standard, preveč kompleksen za praktično uporabo.

4 GLAVNI ELEMENTI INFORMACIJSKE VARNOSTNE POLITIKE

V skladu s standardom[3] dobre prakse za informacijsko varnost (2007) ločimo 6 glavnih aspektov oz. elementov informacijske varnosti, ki podpirajo ključne poslovne procese v organizaciji.

1. Varnostno upravljanje
2. Aplikacije ki so ključne za poslovanje
3. Računalniške inštalacije
4. Omrežje
5. Razvoj programske opreme
6. Okolje končnega uporabnika

4.1 Upravljanje varnosti

Za učinkovito varnost so potrebne jasne usmeritve vodstva organizacije. To področje zajema »top management« v podjetju, ki odloča o varnostni politiki in drugih pravilih, ki morajo biti zavezujoča za vse zaposlene in tiste, ki imajo dostop do informacij in sistemov v neki organizaciji.
Vodstvo se mora zavedati pomena celovite varnostne politike kot pomembnega elementa v podjetju, kar pomeni da mora ustvariti pozitivno razpoloženje v odnosu do informacijske varnosti. Tretje osebe

[3] Standard of good practice for information security 2007, ki ga je izdelal ISF - information security forum.

morajo dobiti občutek, da ima podjetje resen in profesionalen odnos do varnostnih vprašanj. Vodstvo mora prav tako zagotoviti ustrezen sistem odgovornosti in nadzora, ki morata biti sorazmerna z grožnjami. Zaželena je vzpostavitev kriterijev za dostop do informacij in sistemov. Ker imajo managerji omejen čas, znanje in resurse, je priporočljivo da ima podjetje posebno odgovorno osebo, katere delo se bo nanašalo izključno na informacijsko varnost. To je lahko »vodja informacijske varnosti«, ki je tudi odgovorna oseba za varnost. Za lažji pregled nad varnostjo v podjetju je priporočljivo sestaviti »varnostni odbor«, ki ga lahko sestavljajo predstavnik vodstva (npr. član uprave), vodja informacijske varnosti, vodja računalniškega centra, pravni strokovnjak etc. Odbor se nato sestaja kot velevajo potrebe, ter tako ocenjuje dosedanje delo in planira delo v bodoče.
Pomembne naloge vodstva podjetja so tudi odreditev ustreznega budgeta za informacijsko varnost, seznanjenost z aktualnim stanjem o varnosti v podjetju in seveda sprejem ustreznih pisnih dokumentov, kot so varnostna politika v podjetju, strategija informacijske varnosti in drugi akti.
Ko vodstvo sprejme varnostno politiko, je priporočljivo da dokument izda v pisni obliki, tako da bo dostopen vsem zaposlenim na katere se nanaša. Ko je politika sprejeta, je potrebno zaposlene z njo seznaniti. Varnostna politika mora biti skladna z drugimi politikami v podjetju (npr. finančno, zdravstveno, etc.), redno preverjana in posodobljena glede na potrebe in grožnje. Albright (2002) meni, da dobro varnostno politiko določajo:

- jasnost in nedvoumnost,
- uporabnost v praksi,
- določena odgovornost uporabnikov, skrbnikov in managementa,
- uravnoteženost varnosti in produktivnosti,
- predvideno ravnanje v primeru varnostnega incidenta,
- politiko je sprejelo vodstvo podjetja, »top management«.

Pomemben vidik je seznanjanje zaposlenih z varnostno politiko in varnostno ozaveščanje. Tako se lahko pripravijo predavanja, delavnice, brošure, letaki, ki opozarjajo in seznanjajo ljudi o pomenu varnosti in varnostne politike v podjetju. Le tako bo varnostna politika lahko ustrezno zaživela in bo tudi učinkovita. Ljudje morajo informacije naprej ponotranjit, šele na to se bodo tudi »varno vedli«.
Dobra varnostna politika mora zagotoviti klasifikacijo kritičnih informacij, dodeljevanja dostopa in s tem onemogočiti nepooblaščen dostop, analizo tveganja, skladnost s pozitivno evropsko in domačo zakonodajo, kakor tudi mednarodnimi standardi, preprečiti uporabo informacij za namene ki se ne nanašajo na delo in podjetje, preprečiti uporabo in reprodukcijo prepovedane vsebine, preprečiti nepooblaščeno kopiranje informacij ali programske opreme ter preprečiti zlorabo gesel in uporabniških imen.

4.2 Ključne poslovne aplikacije

Gre za zelo pomemben aspekt, saj izguba zaupnosti, integritete ali dostopa do informacij lahko pomeni velik udarec za podjetje. Prince (2009) navaja največje grožnje informacijski varnosti v letu 2010. Sem uvršča škodljivo in zlonamerno programsko opremo, »škodljive« posameznike ki s svojim namernim delovanjem povzročajo škodo podjetju, varnostne luknje v programski opremi, neodgovorne zaposlene, mobilne naprave (npr. GSM) ki omogočajo številne zlorabe, socialna omrežja, socialni inženiring in spletno vohunjenje. Vsa omenjena dejanja imajo pogosto enako posledico, takšno ali drugačno škodo za podjetje. Tako lahko rezultirajo v padcu prodaje, izgubi naročil, pogodb in strank, padcu delnic, izgubi nadzora nad podjetjem, izgubi konkurenčnosti, izgubi zaupanja strank in poslovnih partnerjev, izgubi ugleda, padcu produktivnosti ali celo poškodbi in smrti zaposlenih.
Vprašanje ki se postavlja je, kako vse to preprečiti ali vsaj zmanjšati verjetnost teh pojavov in posledic? Da bi omejili neželene posledice različnih groženj, je potrebno aplikacije ustrezno zavarovati. Tako se omeji dostop do aplikacij, pomembnih za poslovanje samo določenim osebam oz. tistim, ki aplikacije potrebujejo pri svojem delu. Gre za dodelitev posebnih uporabniških imen in gesel za dostop. Istočasno se uvede ustrezna protivirusna zaščita, požarni zid, ustvarjanje varnostnih kopij vseh potrebnih informacij (»backup«), dnevnik dogajanja in dostopa, zaznavanje nepooblaščenega dostopa in odliv informacij, ter drugi postopki. Spet je najpomembnejši vidik ustrezna ozaveščenost uporabnikov aplikacij, saj ravno ti pogosto predstavljajo šibko točko v varnostnem sistemu. Tako se

uporabnike aplikacij izobrazi o pomenu varnosti, lahko v okviru posebnega tečaja ali brošur. Seznani se jih s pravicami in dolžnostmi ki se nanašajo na varno uporabo aplikacij (kot so odjavljanje z računalnika po končani uporabi; shranjevanje spominskih medijev na varnih mestih; varovanje informacij tudi izven delovnega mesta) in sankcijami, v primeru neupoštevanja pravil in neodgovornega ravnanja. Še vedno pa velja, da je veliko učinkovitejša ustrezna preventiva kot grožnje z rigoroznimi sankcijami, saj so le te zgolj odziv na že povzročeno škodo ali neželeno posledico.

4.3 Računalniške inštalacije

Računalniška strojna oprema oziroma tako-imenovan »hardware« predstavlja osnovo, ki poganja vse poslovne aplikacije. Priporoča se, da se za vso računalniško opremo vodi ustrezna inventarna evidenca. Evidenca naj vsebuje specifičen opis strojne in programske opreme, različico opreme in lokacijo, kjer se ta oprema v podjetju ali izven njega nahaja. Podobno kot to velja za aplikacije, je tudi strojno opremo potrebno zavarovati. Uporabljamo nadzor dostopa do računalnikov, kriptografski nadzor (zaščitene datoteke; preverjanje avtentičnosti uporabnikov), zavarovanje pred zlonamerno programsko opremo (kot so črvi, virusi, trojanski konji, vohunski programi), varnostno kopiranje podatkov in redno vzdrževanje računalniške opreme. Potrebno je zagotoviti nemoteno in neodvisno delovanje posameznih računalnikov, da izpad enega računalnika ne pomeni izpad celotnega računalniškega sistema v podjetju.
V zadnjem času smo priča uporabi velikega števila različnih spominskih medijev. Tudi te je potrebno zavarovati z gesli ali pa omogočiti branje le-teh samo na računalnikih znotraj podjetja. Izguba dragocenih informacij iz takih medijev lahko povzroči veliko škodo podjetju.
Prav tako je pomembno, da se podjetje odloči za nakup zanesljive strojne opreme, pri preverjenih prodajalcih, ki nudijo vzdrževanje in kvaliteten servis opreme. Priporoča se uporaba UPS sistemov brezprekinitvenega napajanja in posebnih filtrov proti udaru strele.

4.4 Omrežje

Računalniška omrežja služijo izmenjavi informacij in predstavljajo kanal za dostop do informacij. Po svoji naravi so zelo ranljiva za motnje in različne zlorabe, saj povezujejo različne sisteme med seboj. Osebje ki bdi nad delovanjem omrežja mora biti dovolj kompetentno, da zagotavlja nemoteno delovanje, mora se znati soočiti z izpadi in motnjami, ter se prilagajati nepričakovanim okoliščinam. Za to je pomembno da imamo dovolj ljudi, ki se ukvarjajo s tem področjem. Številčna podhranjenost onemogoča ustrezen nadzor in upravljanje omrežja, pa najsi bo osebje še tako strokovno podkovano in kompetentno.
Pri oblikovanju omrežja, ne gre pozabiti na njegovo obliko, ki mora zadostiti potrebam uporabnikov, zagotoviti se mora kompatibilnost z drugimi omrežji, namestiti primerne požarne zidove, omejiti vstopna mesta v omrežje in preprečiti nepooblaščen dostop do omrežja. Omrežje mora biti zasnovano tako, da zadosti »prometu« oz. pretoku informacij. Tako lahko imamo solidno zavarovana omrežja, ki pa pokleknejo pod težo prevelika prometa. Temu pogosto botruje nepotreben promet, kot so recimo nepooblaščen dostop in koriščenje omrežja s strani tretjih oseb, ki lahko preobremenijo sistem. V času brezžičnega prenosa informacij je pozornost potrebno nameniti tudi temu področju in omrežje ustrezno zavarovati pred nepooblaščenim brezžičnim dostopom s posebnimi gesli in uporabniškimi imeni. Če hočemo da omrežje nemoteno teče, ga je potrebno nenehno nadzorovati. Tako nadziramo morebitne DOS napade, spremljamo sumljive aktivnosti, poskuse vdorov in nepooblaščenih dostopov. Zagotoviti moramo, da spremembe in konfiguracijo omrežja opravlja izključno za to delo pooblaščena in kompetentna oseba.

4.5 Razvoj programske opreme

Kadar sami razvijamo programske sisteme si velja zapomniti, da je implementacija varnostnih mehanizmov v sistem že med samim razvojem učinkovitejša, pa tudi cenejša kot kasneje, ko je sistem že razvit in postavljen. Če je le možno, na vsakem koraku načrtovanja sistemov pomislimo in upoštevamo tudi varnostni aspekt. Najbrž ni potrebno poudarjati, da si nihče ne želi nestabilnih in

»luknjastih« sistemov, ki so lahka tarča napadalcev in zlonamerne programske opreme. Pri razvoju programske opreme ki jo bomo uporabljali v poslovnih procesih ne smemo pozabiti, da bo le ta skladna z varnostno politiko v podjetju, standardi in pravili.

4.6 Okolje končnega uporabnika

Zadnji a nikakor najmanj pomemben aspekt informacijske varnosti v podjetju je končni uporabnik. Zaposleni pri svojem delu uporabljajo poslovne aplikacije, dostopajo do omrežja, uporabljajo strojno in programsko opremo, uporabljajo pomembne poslovne informacije in vse to lahko pomeni tveganje za informacijsko varnost v podjetju. Uporabnike se zato seznani, da je prepovedana nepooblaščena uporaba sistemov in informacij, uporaba informacij in sistemov za druge namene ki ne zadevajo dela, prenašanje nedovoljene vsebine iz svetovnega spleta, razkrivanje zaupnih informacij tretjim osebam in druga pravila. Seveda se spet dotaknemo zelo pomembnega vidika, to je ozaveščanje uporabnikov. Potrebno jim je povedati kaj se od njih pričakuje, kakšne so njihove pravice in dolžnosti glede informacijske varnosti. Podjetja tako v praksi nemalokrat že v pogodbi o zaposlitvi ali pa s podpisom posebnih obrazcev prisilijo posameznika, da se vede odgovorno in varno.
Vsekakor je potrebno, da se posameznikom dodelita njihovo lastno uporabniško ime in geslo za dostop do omrežij, aplikacij in sistemov. Vsakemu uporabniškemu imenu se dodelijo ustrezne pravice, v skladu z delom ki ga upravlja. Tako preprečimo dostop do tistih informacij, ki jih posameznik pri svojem delu ne potrebuje. S tem omejimo možnost zlorabe ali odliva pomembnih informacij iz podjetja. Ob vsem velja zapisati, da je ravno ozaveščenost posameznika o pomenu varnosti tisti ključni element. Zato je pomembno, da se v podjetju ustvari nekakšna »varnostna klima«, kjer se vsi vedejo varno in se zavedajo pomena informacijske varnosti za podjetje.

5 ZAKLJUČEK

Varnostna politika informacijskega sistema je dokument, ki podrobno opredeljuje vsa področja varovanja informacijskega sistema in kot takšna mora biti obvezujoča za vse zaposlene v podjetju. Le tako bo tudi učinkovita. Kvalitetno varnostno politiko pa zagotavlja skladnost le-te z mednarodnimi standardi ISO 17799:2000 (ISO 27002:2005), in ISO 27001:2005, ki jasno določajo najboljšo prakso s področja informacijske varnosti in razlagajo, kaj podjetje potrebuje za skladnost s standardi.
Kot smo lahko videli v članku, so varnostne grožnje s katerimi se soočajo podjetja, realne in še naraščajo. Omrežja, informacije, strojna in programska oprema ter drugi segmenti se kažejo kot precej ranljivi. Raziskava o varnosti informacijskih sistemov je pokazala, da se velika večina podjetij sooča s takšnimi ali drugačnimi varnostnimi incidenti vsaj enkrat letno. Ob tem prihaja do motenj v poslovanju, izgubi strank, povzroča se poslovna škoda, ki lahko vodi celo v propad podjetja. Zato je učinkovita varnostna politika eden izmed glavnih elementov uspešnega in stabilnega podjetja. Zdi se, da se na zahodu tega dejstva zavedajo veliko bolj kot pri nas, kjer nekatera velika podjetja in ustanove še vedno nimajo vpeljane varnostne politike.

VIRI

Albright, J. G. (2002). The basics of an IT security policy. GSEC Practical Requirement V.1.3. Dostopno na: http://www.giac.org/certified_professionals/practicals/gsec/1863.php [17.04.2011]

Barman, S. (2002). Writing information security policies. New Riders Publishing. Dostopno na: http://books.google.com/books?id=bmRfgGEh2PkC&printsec=frontcover&dq=information+security+policy&hl=sl&ei=p-unTeA6zJs6ro-9hQo&sa=X&oi=book_result&ct=result&resnum=1&ved=0CDIQ6AEwAA#v=onepage&q=information%20security%20policy&f=false [12.04.2011]

Frešer, M. (2009). Vpeljava standarda ISO 17799 na rektoratu Univerze v Mariboru. Diplomsko delo, Maribor, Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko.

Information security breaches survey 2010. Technical report. Dostopno na: http://www.infosec.co.uk/files/isbs_2010_technical_report_single_pages.pdf [15.04.2011]

Ključevšek, R. (2002). Standard za varnost. Sistem - revija Monitor. Ljubljana, Infomediji, št. 9, sep. 2002, str. 18-19.

Kosutic, D. (2010). ISO 27001 vs. ISO 27002. Infosec island. Dostopno na: https://www.infosecisland.com/blogview/8055-ISO-27001-vs-ISO-27002.html [19.04.2011]

Martin, C. R., Weise, J. (2001). Developing a security policy. Sun Microsystems. Dostopno na: http://www.sun.com/blueprints/1201/secpolicy.pdf [12.04.2011]

Prince, K. (2010). Top 10 information security threats of 2010. Network security edge. Dostopno na: http://www.networksecurityedge.com/content/top-10-information-security-threats-2010?page=4 [20.04.2011]

Štrakl, M. (2003). Varnostna politika informacijskega sistema. Štirinajsta delavnica o telekomunikacijah VITEL. Brdo pri Kranju, 19. in 20. maj, 2003. Dostopno na: https://lms.uni-mb.si/vitel/14delavnica/clanki/marjan_strakl.pdf [11.04.2011]

The standard of good practice for information security. Information security forum, 2007. Dostopno na: https://www.securityforum.org/about/sampledocuments/downloadsogp/ [18.04.2011]