

Podatki o avtorju: mag.Marjeta Horjak

MFC&L d.o.o.

Linhartova3a, 1000 Ljubljana, Slovenija

Tel.: 01 / 430 74 70

Fax: 01 / 430 74 75

E-mail: marjeta.horjak@mfc-l.si

VPLIV VARNE INFORMACIJSKE TEHNOLOGIJE NA EKONOMSKO USPEŠNOST PODJETJA

POVZETEK

V podjetju obstajajo tehtni in utemeljeni razlogi za postavitev varnega informacijskega sistema, ki vpliva na njegovo ekonomsko uspešnost in konkurenčno prednost predvsem zato, ker Slovenija z vstopom v Evropsko unijo vstopa na globalni trg in podjetja se morajo toliko bolj zavedati posledic morebitnih in nepričakovanih zastojev informacijskega sistema zaradi izrednih okoliščin, npr. večjih izpadov električne energije, požarov, naravnih nesreč ali katastrofalnih napak. Zato mora podjetje zagotoviti normalno delovanje po nepričakovanem in uničujočem dogodku v najkrajšem možnem času.

Ključne besede: varovanje informacij, varnostni standardi, varnostna politika podjetja, informacijski sistem.

ABSTRACT

In the company exist cogent and well-founded reasons for implementation of the safe information system which has influence on company's economic efficiency and competitive advantages. Especially now when Slovenia as EU member enters the global market the companies should be more aware of the consequences of unexpected blockage of the information system due to emergency circumstances such as cutout of the circuit on the large scale, fires, natural catastrophes or huge mistakes. Therefore the company must assure working process after the unexpected and destructive event in the shortest possible period of time.

Key words: the information security, the safety standards, the information policy of the company, information system

1. UVOD

V članku bom poskušala predstaviti vpliv varne informacijske tehnologije na ekonomsko uspešnost podjetja. Tudi na podlagi opravljene ankete o pomembnosti uvajanja varnega informacijskega sistema v zagotavljanju konkurenčne prednosti podjetja, ki je pokazala, da slovenska podjetja vsako leto bolj sledijo varnostnim standardom, zakonodaji in postavitvi preglednih in varnih sistemov, predvsem zaradi potreb po racionalizaciji in avtomatizaciji poslovanja. To pa predstavlja zahtevno in odgovorno opravilo ter nenehno investicijsko vlaganje v ljudi, izobraževanje, poslovne procese, računalniško in varnostno tehnologijo.

2. VLOGA IN POMEN INFORMATIKE V PODJETJU

Razlogov, zakaj uvajati sisteme varovanja poslovnih informacij, je več, npr. preprečevanje vdorov v strogo varovane računalniške sisteme in preprečevanje kraje pravic intelektualne lastnine ter zaščita sistema pred virusi. Z uvedbo sistema varovanja informacij pa podjetje lahko ohranja

konkurenčno prednosti in obstoj na svetovnem trgu, zato je pomembno, da podjetja v sistemu varovanja poslovnih informacij vidijo tudi **poslovno priložnost**. Obvladovanje **tveganj**, povezanih s človeškimi dejavniki, računalniškimi sistemi in tehnologijo, naravnimi vplivi okolja in obvladovanje tveganj izvedbe poslovnih procesov, so dovolj tehtni razlogi, da bi odločitev o uvedbi sistema varovanja poslovnih informacij moralo sprejeti vsako podjetje, katerega cilj je poslovati kakovostno, uspešno in učinkovito, predvsem pa dolgoročno.

Pomembno je, da varnostne zahteve podjetja nastanejo kot posledica poslovnih zahtev in

- zagotavljajo učinkovitost poslovanja,
- sledijo zakonskim in pogodbenim zahtevam,
- zagotavljajo zmanjševanje tveganj v podjetju.

Glavni razlog za obvladovanje **informacijskih tveganj** je poslovne narave – kontinuiteta **zagotavljanja informacij**, ki predstavljajo **konkurenčno prednost** podjetja.

Zato so velika podjetja še bolj izpostavljena napadom s strani konkurence kot tudi drugih **napadalcev**, še posebej, če se ukvarjajo z izdelki visoke tehnologije, ki na trgu prinašajo velike dobičke, npr. Lek, Krka. Posledice zaradi morebitnega vdora v informacijski sistem, nedelovanje poslovnih funkcij, napake in nepravilnosti pri poslovanju lahko zelo hitro ogrozijo obstoj podjetja na domačem in svetovnem trgu.

Informacije so namreč vedno bolj pomemben dejavnik uspešnega delovanja podjetja, zato moramo vzpostaviti ustrezne **sisteme varovanja informacij** na temelju varnostnih standardov, zakonodaje in razpoložljive informacijske tehnologije. Le-ta pa koristi svojemu namenu, če jo uporabljamo na primeren ter pravilen način, da nam prinaša koristi (zmanjšuje stroške in povečuje produktivnost). V večini primerov se uporablja kot orodje za upravljanje z informacijami, zato moramo zagotoviti, da tehnologija omogoča **zaupnost, celovitost in razpoložljivost informacij**.

Glavni cilji vzpostavitve ustreznih sistemov varovanja informacij v podjetju so podobni ciljem uvajanja sistema **kakovosti**, in sicer:

- **učinkovito zadovoljevanje potreb poslovnih partnerjev (Patru 2003:32)**, tako da so jim storitve na voljo v skladu s kriteriji kakovosti in varnosti, ki jim jih podjetje obljublja,
- **obvladovanje lastnih poslovnih procesov (Patru 2003:32)** in dejavnikov, ki omogočajo njihovo izvedbo (tehnologija, kadri, informacije),
- **stalno izboljševanje kakovosti in varnosti poslovanja (Patru 2003:32)**, npr. z dobro varnostno politiko podjetja, ki ureja strategijo izvajanja informacijske varnosti,
- **zmanjševanje poslovnih in operativnih tveganj (Patru 2003: 32)**, npr. z uvedbo informacijskih sistemov za neprekinjeno delovanje, ki podjetju ohranjajo kontinuiteto zagotavljanja informacij.

Sistem in procesi varovanja informacij morajo temeljiti na **jasni zakonodaji, standardih**, ki so v uporabi, predvsem pa **zavesti in visoki stopnji** zaupanja v poslovanje.

V tujini si veliki poslovni subjekti z objavo **lastne varnostne politike**, torej tiste, ki jo uporabljajo znotraj podjetja, pridobijo velik ugled (Valenčič 2000: 173, Brenton 1999: 15-38 in Parker 2001: 43-44). Informacija o večletnem nemotenem poslovanju podjetja kaže na njegovo zrelost in dobro upravljanje. Prav tako je pokazatelj dobrega upravljanja, če v podjetju obvladajo **poslovne in tehnološke** vidike varovanja informacij, če je razvita organizacijska in informacijska kultura ter kultura upravljanja s tveganji.

Vpliv varne informacijske tehnologije na ekonomsko uspešnost in konkurenčno prednost podjetja lahko ponazorim tudi z naslednjimi primeri:

- Dokler neko npr. letalsko podjetje, nima varne informacijske tehnologije, kot jo imajo konkurenčni letalski prevozniki, ki so na trgu, na trg ne more vstopiti.
- Z varno informacijsko tehnologijo je mogoče **ustvariti nove storitve**, ki jih ne more nuditi

podjetje, ki nima enake tehnologije (npr. v zdravstvenih organizacijah - elektronska izmenjava podatkov, v bankah- elektronski plačilni sistem).

- Kupec, ki uporablja varno računalniško izmenjavo podatkov, lahko od dobavitelja zahteva, da jo mora vpeljati, če hoče ostati dobavitelj še naprej. Pri tem pa mu določa tehnološke pogoje (Možina 1994: 730-731), npr. varnostni standard ISO17799/BS 7799

3. Varnostni standard ISO17799/BS7799

Varnostni standard ISO17799/BS7799, kot eden od temeljev, ki pomembno vpliva na izboljšanje informacijske varnosti uporabljajo podjetja pri pripravi in implementaciji informacijskih varnostnih politik, postopkov in procedur. Zaradi **celovite obravnave informacijske varnosti** ima ta standard pomen pri doseganju uspešne varnostne politike podjetja.

Upoštevanje določil standarda ter prednosti vzpostavitve STANDARDA BS7799 /ISO 17799 so predvsem naslednje:

- **ZAUPNOST INFORMACIJ** – določena informacija je dostopna samo tistemu, ki mu je namenjena,
- **CELOVITOST INFORMACIJ** – točnost in popolnost informacije ter metode obdelave,
- **DOSTOPNOST INFORMACIJ**- da imajo avtorizirani uporabniki dostop do informacije in s tem povezanih sredstev, kadarkoli je potrebno (www.iziv.org, 20.04.2004).

V Sloveniji je certifikat ISO 17799 & BS7799 **pridobilo** podjetje Razvojni center IRC Celje.

Velja omeniti zahtevo pri veliko mednarodnih javnih naročilih, ki omenjajo pogoj, da mora podjetje, ki želi kandidirati na javnem naročilu in pridobiti posel, imeti vzpostavljeno politiko varovanja informacij in tudi certifikat BS7799/ISO 17799. Če želijo gospodarske družbe poslovati s tujimi podjetji na enakovreden način bodo morale pridobiti omenjeni certifikat.

Tudi Banka Slovenije je konec leta 2003 izdala Sklep o določitvi pogojev, ki jih mora izpolnjevati banka oziroma hranilnica za opravljanje bančnih oziroma drugih finančnih storitev (Uradni list RS, št. 124/03), ki v 2.b členu določa:»Banka mora v svojem poslovanju upoštevati slovenska standarda SIST BS7799-2:2003 in SIST ISO / IEC 17799:2003.« Banke morajo najprej oceniti tveganje in grožnje ter analizirati svoje poslovanje. Nato pa se odločijo, katere kontrole, ki jih določa standard, bo uvedla.

Vlada RS je že zadolžila ministrstva in organe v sestavi ministrstva, da pripravijo varnostno politiko na osnovi priporočil ISO17799. Državne uprave vodilnih držav članic EU, kot so Nemčija, Velika Britanija in Francija, že vpeljujejo politiko varovanja informacij kot določa navedeni standard.

Prav tako se v slovenskih **zdravstvenih organizacijah** (zdravstveni domovi, bolnišnice) zavedajo, da je stanje varovanja informacij neustrezno in ponekod kritično, zato je trend, da zdravstvene organizacije v Sloveniji sprejmejo poenoteno politiko zagotavljanja varnosti in informacij v skladu z mednarodnim standardom ISO 17799 (Rudel 2004:16). Sprejeta varnostna politika pa bi omogočila vključitev zdravstvenih organizacij v **nacionalni sistem elektronske izmenjave podatkov med ustanovami**.

V kolikor želimo opredeliti **vpliv** standarda na podjetje, lahko rečemo, da podjetja, ki bodo svoje delovanje uskladile s standardom, imele **prednost pri sklepanju novih poslov tako doma kot v okviru Evropske unije, prav tako pa tudi v poslovanju z drugimi državami v svetu**, zato lahko štejemo, da so prednosti podjetij ob uporabi varnostnih standardov naslednje:

- **Konkurenča prednost**; pridobljen certifikat tujim podjetjem olajša odločitev za sodelovanje s slovenskimi podjetji, ki jih še ne poznajo.
- **Ekonomska prednost** z vidika povečanja prodaje storitev in zmanjšanja stroškov.
- **Ugled** podjetja.

- *Zaupnost, celovitost in razpoložljivost informacij.*
- *Obvladovanje tveganj.*

4. ZAKLJUČEK

Sklepno lahko zaključim, da se je potreba po jasni informacijski varnostni strategiji v zadnjih letih zelo povečala. Zgolj uporaba varnostnih orodij in zaščita posameznih delov organizacije ni več dovolj. Resnično reševanje problemov informacijske varnosti pomeni zagotavljanje celovite varnostne strategije podjetja.

Posamezniki se odločamo za sklenitev življenjskega, nezgodnega, avtomobilskega zavarovanja, vendar vedno z mislijo, da tega najverjetneje ne bomo potrebovali. Podobna filozofija, zavarovanje podjetja pred izgubo podatkov in njihovim razkritjem, mora veljati tudi pri podjetju.

Informacijska varnost je proces, ki nas ščiti pred naraščajočim in nevarnim kriminalom.

LITERATURA:

- Brenton, Cris (1999) *Mastering Network Security*. Alameda California: Sybex Network Press Inc.
- *Možina, Stane (1994) Management*. Radovljica: Didakta
- *Parker, Robert G. (2001) Creating the Privacy Compliant Organization, Information Systems Control Journal*
- *Patru, Primož (2003) Ukrepi v primeru informacijskih nesreč. Šempeter pri Gorici: Inštitut IZIV*
- *Rudel, Drago v Varnostni forum (Šinigoj, Aleksander), julij-avgust 2004 str. 16*
- *Sklep Banke Slovenije, Uradni list RS, št. 124/03*
- *Valenčič, Iztok (2000) Postavitev in uvedba dobre varnostne politike, Mednarodna konferenca o revidiranju in kontroli informacijskih sistemov – zbornik referatov*

VIRI IZ MEDMREŽJA:

- *Information Security Management Systems ISO/IEC 17799&BS7799 Part 2, <http://www.xisec.com/>, 16.08.2004*
- *www.palsit.si, 20.08.2004*
- *INŠTITUT IZIV: www.iziv.org, 20.04.2004*