Ocena tveganj za bolnišnico Golnik

Žiga Trdina, Fakulteta za organizacijske vede, Univerza v Mariboru.
Igor Bernik, Fakulteta za varnostne vede, Univerza v Mariboru.

Namen in cilj prispevka
Glavni namen prispevka je povečanje zavedanja varovanja informacij v skladu s standardom ISO/IEC 27001 ter prikazati način izdelavi ocene tveganj po kvalitativni metodi, ki bi lahko služila kot osnova izdelave ocene v primerljivih primerih.

Metodologija
Uporabljena je deskriptivna metoda za pristop k študiji. Na podlagi zbranih načinov ocenjevanja tveganj, smo se osredotočili na proces informacijskega sprejema in obravnavanja pacienta v bolnišnici Golnik. Popisali smo najnujnejša informacijska sredstva, ki morajo biti v tem času dosegljiva ter s pomočjo kvalitativne metode določili tveganje podjetja. Končni rezultat študije služi kot osnova izdelave analize tveganj v primerljivih poslovnih sistemih.

Ugotovitve in omejitve
Raziskava je bila narejena v bolnišnici Golnik- Kopa. V našem primeru smo izhajali iz pacienta in sicer , katera informacijska sredstva morajo biti dosegljiva, ko računalniško sprejmemo pacienta v bolnišnico, premestimo na oddelek, predpišemo dieto, preverimo zavarovanje, obračunamo, hkrati pa se morajo vse informacije beležiti na strežnik in biti dosegljive vsem uporabnikom, ki z njimi razpolagajo. Ali v obratnem vrstnem redu, kako bi potekalo poslovanje v podjetju v primeru odpovedi ključnega sredstva. Kakšen bi bil odzivni čas, postavitve nadomestnega ter kako bi se odzvalo vodstvo v primeru nekonkurenčnega poslovanja ter kakšne posledice bi to povzročilo podjetju. Vse to so vprašanja, ki se jih velikokrat ne zavemo, dokler ne pride do resnih težav.

Izvirnost Strokovni prispevek bo pripomogel k boljšemu razumevanju vzpostavitve sistema upravljanja in varovanja informacij oziroma ocene tveganj.

Ključne besede: ocena tveganj, grožnje, varovalni ukrepi, informacijska varnost, bolnišnica

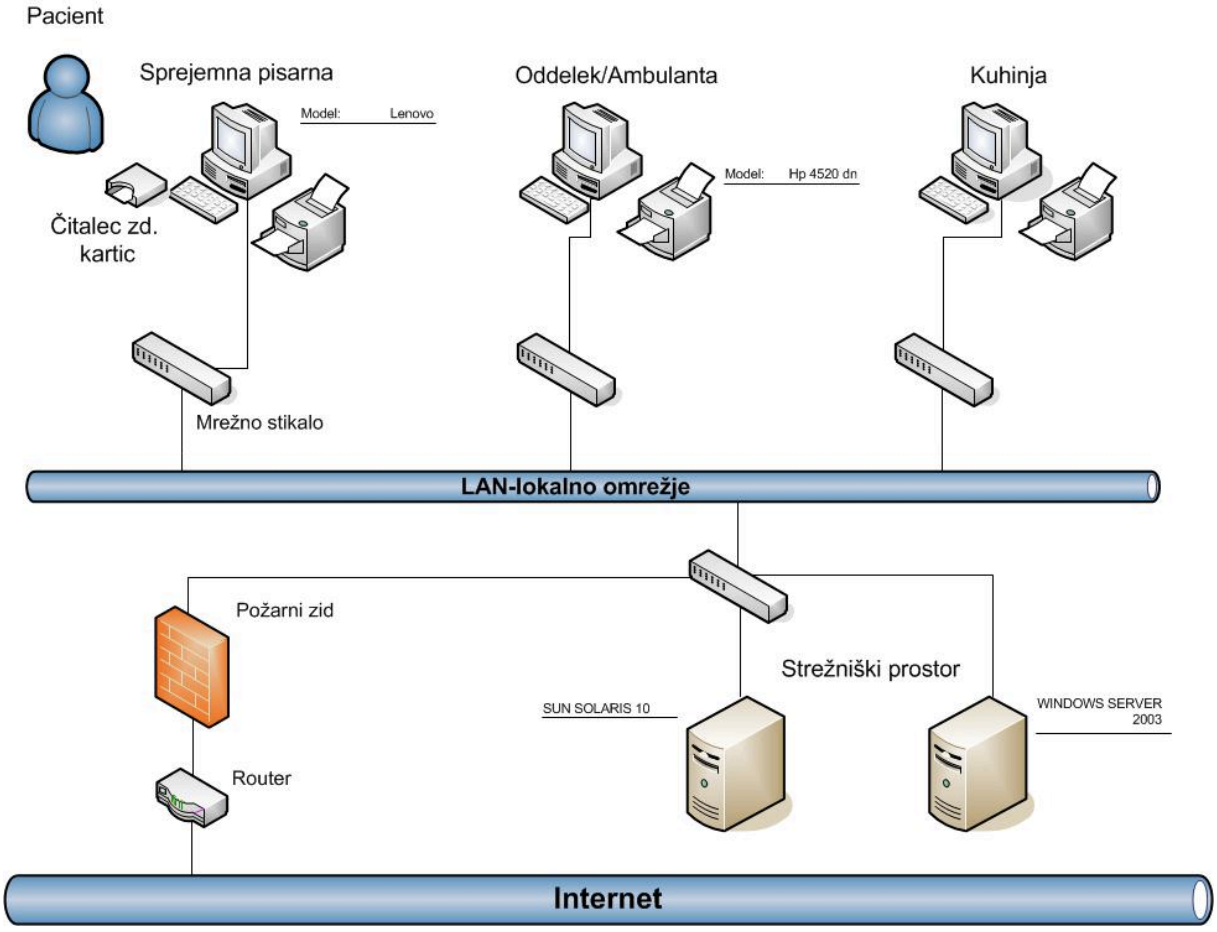
1 UVOD

Dandanes se podjetja pri poslovanju zanašajo na notranje računalniške sisteme in povezavo z internetom. Pri tem si ne morejo privoščiti prekinitve poslovanja. Spremembe in razvoj na področju informatike vedno znova in znova zahtevajo neprestano pozornost organizacije. Dinamičnost v razvoju tehnologije, ozaveščenost, zahteve vodstva in strank, hitre spremembe na pravem področju in kompleksnost sistemov zahtevajo znanje. Zaradi vse večje zapletenosti, neobvladljivosti informacijskih sistemov in računalniških tehnologij se pojavlja potreba po zaščiti in zagotavljanju varnosti. Varnostni incident ima lahko širše negativne posledice na dohodke podjetja, zaupanje strank in stike z javnostjo. Zaradi teh posledic je varnost informacij pomemben sestavni del učinkovite poslovne strategije (Egan, 2004). Razprave o tem, kakšna je dejanska varnost in pomen informatike v podjetju, so vse pogostejše, poleg tega statistika dokazuje, da vsako leto prihaja do večjega števila okužb s zlonamerno programsko kodo, kraj, zlorabe podatkov ter ostalimi nezaželenimi dogodki, ki lahko škodujejo podjetju. Zagotavljanje varnosti pomeni uvajanje ustreznih varnostnih mehanizmov oziroma varnostnih kontrol v poslovne procese organizacije. Organizacije morajo doseči raven zaščite, ki jim omogoča racionalno uporabo informacijskih sredstev ter onemogoča morebitne varnostne incidente, povezane z varovanjem informacij (Whitman in Mattord, 2003). Avtorja meniva, da se veliko podjetij ne zaveda ranljivosti informacijskih sistemov in, da temu posvečajo premalo pozornosti (Bernik in Prislan, 2011). V večini primerov se skrbniki informacijskih sistemov preveč zanašajo na programsko ali fizično varnost, kot so: požarni zidovi, antivirusne zaščite, sistemi za preprečevanje vdorov ter druge oblike varnostnih mehanizmov. Iz tega velikokrat sklepajo, da je varnost v podjetju ustrezna, ne pomislijo pa, da je lahko prav človeški faktor največji povzročitelj groženj, ki lahko

škoduje podjetju. Skratka eden iz med načinov, da organizacija zagotovi ustrezno stopnjo varnosti v lastnemu informacijskemu sistemu je, da se grožnjam zoperstavlja. To počne v procesu upravljanja s tveganji (Bernik in Prislan, 2011).

2 POSTOPEK IZDELAVE

Za uspešno poslovanje bolnišnice je najpomembnejše načelo kakovosti, razpoložljivosti in varnosti podatkov v vseh pogojih, pri tem pa se mora podrejati področni zakonodaji. Poleg tega se bolnišnice vključujejo v projekt združenja zavodov Slovenije (Znet, 2011) ta pa zahteva vzpostavitev sistema varovanja informacij v celotni ustanovi. Če smo želeli zadostiti vsem zgoraj omenjenim merilom smo se morali soočiti z upravljanjem tveganj v bolnišnici.
Celovito upravljanje s tveganji pomeni sistematičen pristop k strukturiranju in definiciji prioritet pri izgrajevanju celovitega varnostnega sistema. To pomeni, da je zelo pomembno, da pri ocenjevanju tveganj najprej določimo ustrezno usposobljeno ekipo, ki bo znala pridobiti informacije v sodelovanju z zaposlenimi na vseh nivojih ter, da točno opredelimo najnujnejše procese, ki jih želimo obravnavati (S&T, 2011). Bolnišnica je ustanova, kjer je na prvem mestu zdravje pacienta. Zato prikazujemo primarni proces sprejema pacienta v bolnišnico, ki je tudi ključen za reševanje njegovega bolezenskega stanja.



Slika 1: Shematični prikaz sprejema pacienta v bolnišnico (vir: lasten)

Na podlagi slike 1 smo v prvem koraku popisali najnujnejša informacijska sredstva, ki morajo biti dosegljiva v času sprejema in obravnavanja pacienta. V ta del smo vključili delovne postaje zaposlenih, prenosnike, čitalce zdravstvenih kartic, tiskalnike, magnetne enote, zunanje medije ter ostale pomembne dobrine. Glavni del opisa je namenjen zavarovanju in tveganju na strežniških sistemih, saj so le ti najbolj izpostavljeni. Prav ti lahko bolnišnici in pacientu v primeru

nerazpoložljivost povzročijo največjo škodo. Hkrati pa se na njih kopiči veliko število podatkov, zato morajo biti ustrezno zanesljivi. Tako kot opisujejo Srebrnič, Krkoč, Janezič in Šinigoj (2004), smo omenjene dobrine ločili po skupinah; strojna oprema, programska oprema, podporna oprema, informacije in podatki ter seveda zaposleni. S tem smo povečali preglednost seznama. Poleg tega je smiselno, da vsem popisanim informacijskim sredstvom zapišemo skrbnika in lokacijo sredstva. V primeru obsežnega seznama in odpovedi, točno vedo, kje se to sredstvo nahaja ter kdo je odgovoren za odpravo napake (Zavod za zdravstveno varstvo, 2011). Ko imamo končan seznam, se osredotočimo na vrednotenje dobrine.
Vrednotenje opravimo na podlagi vrednosti posamezne dobrine za organizacijo oziroma vrednost škode, ki bi jo organizacija utrpela v primeru izgube, uničenju, okvari sredstva ali drugih incidentov. Vrednost dobrin ocenjujemo tudi glede na zaupnost, celovitost in razpoložljivost (Berčič in drugi, 2003). Sledi opredelitev groženj. Tu je potrebna posebna pozornost, da zajamemo čim večje število nevarnosti, ki bi v lahko škodile podjetju. Za lažje pomoč pri definiranju teh si lahko pomagamo z različnimi teoretičnimi izhodišči (npr. Whitman in Mattord, 2008). V tretjem in četrtem koraku ocene tveganj, določamo verjetnost uresničitve groženj ter stopnjo ranljivosti dobrin. V tem delu opredelimo kakšna je verjetnost da se posamezna grožnja uresniči ter kakšno imamo trenutno zaščito zoper opisane grožnje.

3 UGOTOVITVE

Z analizo smo ugotovili, da trenutno stanje v bolnišnici ni slabo vendar, da obstajajo določene nevarnosti, ki bi lahko v prihodnje ogrozile zdravstvene procese. Dobljene rezultate smo preučili s pomočjo prevajalne tabele 1.

Tabela 1: Prevajalna tabela za oceno tveganja (vir: Srebrnič in drugi, 2004)

Verjetnost uresničitve grožnje		**N (nizka)**			**S (srednja)**			**V (visoka)**		
Stopnja ranljivosti		N	S	V	N	S	V	N	S	V
Vrednost sredstva	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Za mejno vrednost, smo določili oceno 6. Se pravi, končna ocena, ki vsebuje manjšo vrednost, od zgoraj omenjene, bolnišnici ne predstavlja večje nevarnosti pri poslovanju. V našem primeru smo zabeležili štiri kritična področja, ki smo jih kasneje obravnavali ter jim podali varovalne ukrepe. Ostala sredstva smo glede na predpostavko, da podjetju ne morejo povzročiti večje škode izločili iz območja tveganja. Največje pomanjkljivosti so se pokazale predvsem pri podatkovnem strežniku. Možnost grožnje se pojavila pri poplavi, oz. izlivu vode in odpovedi strojne opreme. Za primer odpovedi strojne opreme smo predlagali postavitev dodatnega strežnika, ki bi varnostno kopiral podatke na oba strežnika hkrati. Postavitev odtočnih kanalov oz. alarmnih naprav pa bi grožnji v primeru izliva vode zmanjšali nevarnost tveganja. Naslednja nevarnost se je pokazala pri neprekinitvenem (UPS) napajanju. Res je da v bolnišnici za dodatno napajanje uporabljamo električni generator, vendar bi bilo v primeru odpovedi naprave, napajanje prekinjeno. S vzporedno vzpostavitvijo dodatnega UPSa pa bi se tveganju izognili. Nevarnost smo opazili tudi pri zunanjih medijih, predvsem USB ključkih. V velikih primerih se medijem povzroča premalo pozornosti, saj so podatki, ki jih zaposleni prenašajo izven bolnišnice nezaščiteni in bi se lahko zlorabili. Vsaka najmanjša površnost, izguba ključka, bi lahko bolnišnici povzročila velike neprijetnosti s strani razkritja pomembnih podatkov. S pomočjo šifriranja pa bi se to vrstnemu tveganju izognili.

Realizacija zgoraj predlaganih ukrepov, bo občutno vplivala na izboljšanje varnosti upravljanja in varovanja informacij. Stroški izvedbe, so zanemarljivi v primerjavi z škodo, ki bi nastala v primeru pojava groženj.

4 ZAKLJUČEK

Obvladovanje tveganj je dolgotrajen proces prepoznavanja ranljivosti lastnega informacijskega sistema katerega uporabljajo uspešne organizacije za doseganje poslovnih ciljev. Prav ta je poleg znanja, kapitala in informacij ključni del pri vodenju podjetja. Glede na dolgoročen in kompleksen proces bi vsaka organizacija morala veliko več svoje pozornosti nameniti vzpostavitvi ustreznega sistema in seveda omogočiti izobraževanja s strani zaposlenih, ki so vključeni v projekt. Zavedati se je potrebno, da z samo analizo ni možno identificirati vsa tveganja, ki bi lahko ogrozila poslovne procese, niti jih izločiti. Z ukrepi je možno tveganje zmanjšati na spremenljivo raven. Poleg tega je zelo pomembno, da podjetja redno izvajajo analize tveganj, preverjajo učinkovitost sprejetih varnostnih ukrepov, redno posodabljajo oceno ter dokumentirajo nastalo gradivo. Na poti do želenih rezultatov je potrebno razumeti, da uvajanje sistema ne bo prineslo želenih sadov brez podpore vodstva, ki pa tu igra ključno vlogo. Ocenjevanje tveganj ni opredeljen kot povsem tehnična funkcija, ki se izvaja le ob pomoči informatikov, ampak se izvaja v celotni organizaciji, oziroma se z njim sooča tudi vodstvo, ki mora podpirati končne odločitve.

VIRI

Bernik, I. in Prislan, K. (2011). Proces upravljanja s tveganji v informacijski varnosti. Prispevek na konferenci. Izvleček pridobljen 25. 10. 2011, s http://www.fvv.uni-mb.si/DV2010/zbornik/informacijska_varnost/Bernik_Prislan%20proces%20upravljanja.pdf.

Berčič, B., Bojanec, A., Krkoč, P., Mrhar, P., Patru, P., Šinigoj, A. idr. (2003). Ukrepi v primeru informacijskih nesreč. Šempeter pri Gorici: Inštitut za informacijsko varnost.

Srebrnič, V., P., Krkoč, Janežič, D., A., Šinigoj. (2004). Grožnje elektronskega poslovanja - upravljanje z informacijskimi sistemi. Šempeter pri Gorici: Inštitut za informacijsko varnost.

S&t, Vzpostavitev sistema vodenja in varovanja informacij. Pridobljeno 1.12.2011, s http://www.snt.si/is/77459.si.php.

Egan, M. in Mather,T. (2005). Varovanje informacij, grožnje, izzivi in rešitve. Vodnik za podjetja. Ljubljana: Pasadena.

Trdina, Ž. (2011). Ocena tveganj informacijskega sistema v bolnici Golnik . Diplomsko delo, Kranj: Univerza v Mariboru, Fakulteta za organizacije vede.

Znet. Pridobljeno 25.11.2011, s http://www.zdrzz.si/informatika/e-zdravje/zNET.

Zavod za zdravstveno varstvo, Implementacija varnostnih politik pri izvajalcih zdravstvene dejavnosti, pridobljeno na izobraževanju v Ljubljani.

Whitman, M., Mattord, J. (2003). Principles of information security. Canada: Course technology.