Register tveganj kot nadzorna plošča upravljanja informacijske varnosti

Branko Cvelbar**,** Ministrstvo za finance-GS-SPA

Namen prispevka: Visoka stopnja uporabe informacijskih tehnologij v javni upravi je prinesla vrsto novih groženj in zlorab. Upravljanje tveganj in zagotavljanje informacijske varnosti postaja pomemben gradnik učinkovitega, varnega in zanesljivega delovanja javne uprave in s tem tudi subjektov nacionalne varnosti. Prispevek želi strokovni javnosti približati nekatere od priložnosti za udejanjanje učinkovitejšega upravljanja informacijske varnosti. Predstavljena je potreba po izgradnji novega modela sodelovanja javne uprave z udejanjanjem večje stopnje medresorskega sodelovanja, izmenjave podatkov in informacij (»need to share«) in izgradnjo (centralnih) registrov tveganj kot nadzorne plošče upravljanja.

Metodologija: Uporabljene bodo metode deskripcije in poizvedovanja. V prispevek so vključene analize izkušenj dobrih (in slabih) praks pri oblikovanju, izgradnji, udejanjanju podpore za odločanje in nadzor upravljanja z viri, ki jih je možno uporabiti pri izboljšanju informacijske varnosti.

Ugotovitve: Temeljna ugotovitev prispevka je, da udejanjanje registrov tveganj in njihovo dopolnjevanje predstavlja proaktivni pristop predstojnikov v javni upravi, za učinkovitejše upravljanje tveganj in s tem vzpostavljanje predpogojev za udejanjanje reform in nujnih strukturnih sprememb. Stanje normativne ureditve informacijske varnosti sledi svetovnim trendom. Na praktičnem področju pa udejanjanje teh standardov in postopkov zahteva višjo stopnjo razumevanja in podpore, ki mora preseči določeno stopnjo ravnodušnosti in pomanjkanja volje najvišjih avtoritet v državi. Mnogi pogrešajo večjo koordinacijo, ki, z omejevanjem vrste virov, postaja nujnost.

Omejitve/uporabnost raziskave: Prispevek obravnava analizo dostopnih informacij pri zagotavljanju informacijske varnosti, iz česar izhaja popoln pregled organizacij in podjetij, ki so že pridobila certifikat ISO 27001 in ISO 27002. Težje je pridobiti informacije, koliko subjektov javne uprave je v posameznih fazah zagotavljanja informacijske varnosti, ki je podlaga za učinkovito in varno delovanje poslovnih obveščevalnih sistemov. Vrsta pridobljenih informacij je obetavna, saj se v javni upravi izvaja vse več varnostnih pregledov in naročil analiz odstopanj od zahtev in priporočil standardov informacijske varnosti.

Praktična uporabnost: Rezultati in praktična uporabnost prenosa dobrih praks z večletnega sodelovanja na velikih medresorskih, interdisciplinarnih projektih so del stvarnosti v posameznih mikro okoljih v javni upravi. Udejanjanje v prispevku podanih priporočil predstavlja možnost za vrsto sinergij in izboljšanja informacijske varnosti na ravni celotne javne uprave. Posamezne spremembe v tej smeri so implicirane v praksi kot pristop k reševanju zahtevnejših in obsežnejših nalog, projektov in prenove poslovanja.

Izvirnost/pomembnost prispevka: Prispevek, z zgledi in ob upoštevanju izkušenj, gradi na zavedanju, da se informacijsko varnost v največji meri zagotavlja z »mehkimi« veščinami v okviru vodenja celotne organizacije in širše v okviru pogodbenih sodelavcev. Tehničnemu področju se velikokrat namenja prevelik poudarek.

Ključne besede: register tveganja, informacijska varnost, kriza, nadzorna plošča, novi poslovni model javne uprave.

1 UVOD

Globalizacija in informatizacije sta prinesli vrsto prednosti, priložnosti, velike odzivnosti in on-line spremljanja in izmenjave podatkov. Na drugi strani pa tudi vrsto novih groženj, ki se lahko pojavijo od kjer koli. Tekma za ohranjanje gospodarske rasti, razvoj in bližnjice do inovacij, patentov, poslovnih skrivnosti in tveganj, dobivajo pospeške na področju ekonomske obveščevalne dejavnosti. Pri tem gre v vrsti držav za najtesneje sodelovanje teh služb in podjetij. To postavlja pred javno upravo zahtevo za pospešeno zagotavljanje visoke stopnje informacijske varnosti in obvladovanja ostalih tveganj. Razsežnost krize in s tem povezanih težav zahteva hitrejše odzivanje in uporabo novih, inovativnih pristopov.
V vrsti informacijsko-komunikacijskih sistemov javne uprave, in s tem tudi subjektov nacionalne varnosti, se zbira, obdeluje, obravnava, izmenjuje in hrani vrsta pomembnih, osebnih, občutljivih in tudi tajnih podatkov. S Strategijo razvoja elektronskega poslovanja ter izmenjave podatkov iz uradnih evidenc – SREP je oblikovan in potrjen pristop za uravnotežen razvoj elektronskega poslovanja v javni upravi in prenos rešitev ter dobrih praks, ki so nastale na področju e-uprave, na druga področja elektronskega poslovanja v javni upravi (SREP, 2011). Sledil je sprejem Priporočil informacijske varnostne politike javne uprave - IVPJU. Navedena priporočila izražajo politiko, s katero želi javna uprava zaščititi informacijsko premoženje, ki ga upravlja. S tem so postavljena osnovna varnostna izhodišča za zaščito informacijskih sredstev pred nevarnostmi, tako notranjimi kot zunanjimi, namernimi ali naključnimi (IVPJU, 2011).
V prispevku je dan poudarek na pregledu stanja na tem področju in iskanju odgovora na vprašanje, kako trdna je informacijsko varnostna veriga v javni upravi. Pri oblikovanju novega poslovnega modela so-delovanja javne uprave, za zagotavljanje informacijske varnosti, se velja opreti na preizkušene in delujoče prakse in pristope. Dolgoletne izkušnje pri razvoju, udejanjanju in stalnem dopolnjevanju ter nadgradnji sistema MFERAC - računalniška podpora enotnemu računovodstvu RS, so zgled dobre prakse in sinergij medresorskega sodelovanja. V prispevku je predstavljenih nekaj tez, ki opredeljujejo pristop in oblike sodelovanja za doseganje zahtevnih finančnih ciljev javne uprave na področju zagotavljanja informacijske varnosti.

2 REGISTER TVEGANJ IN ZAGOTAVLJANJE INFORMACIJSKE VARNOSTI

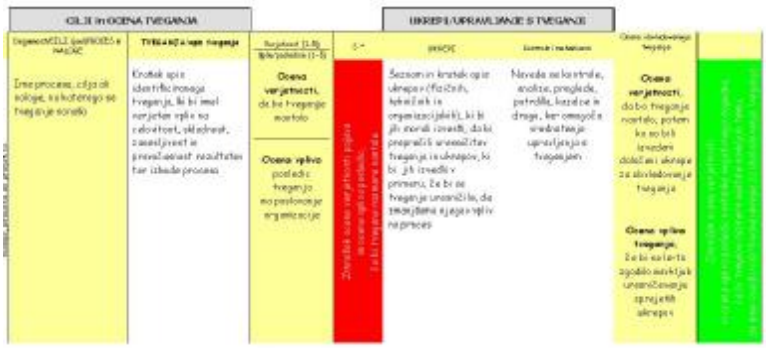
Naloge upravljanja s tveganji definiramo kot stalni proces obvladovanja izpostavljenosti poslovanja tveganjem in omejevanja tveganj na sprejemljivi ravni. To pomeni opredelitev izpostavljenosti tveganju, ovrednotenju ugotovljenih tveganj, razvrstitve po verjetnosti in teži možnih posledic ter na podlagi takšne analize vzpostavitev primernega sistema notranjih kontrol za njihovo obvladovanje.

V podjetju, kjer se vzpostavljajo strategije obvladovanja tveganja, se morajo, še preden se porazdelijo vloge in pooblastila za obvladovanje tveganja, popolnoma razčistiti druge, vodstvene in avtoritativne vloge ter odgovornosti pri poslovanju. Pravilno ovrednotenje trenutnega položaja je za podjetje pri osredotočanju na vzpostavitev strategije obvladovanja tveganja bistvenega pomena, saj pri tem spoznamo oziroma odkrijemo specifične odnose in medsebojne povezave, ki lahko ključno opredeljujejo razplet dogodkov v prihodnosti. Stanje v prihodnosti je zelo verjetno nadaljevanje trenutnega stanja z manjšimi ali večjimi odkloni. Ti odkloni so ponavadi manjši, če predvidevamo stanje v bližnji prihodnosti (Berk, Peterlin in Ribarič, 2005).

2.1 Register tveganj organizacije in vzpostavitev sistema vodenja varovanja informacij

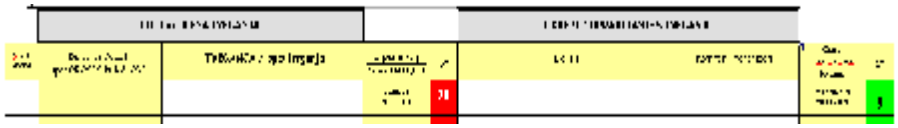
Oblikovan in s ključnimi vodji usklajen (centralni) register tveganj organizacije, posameznih procesov in večjih projektov z dvo-nivojsko strukturo je pregleden, slikovit in analitičen ter celovit pregled upravljanja tveganj: vrsta področij zahteva dodatne procedure in spremljanje skladnosti s področnimi standardi in normativi.

Z vzpostavitvijo in rednim pregledovanjem ter posodabljanjem registra tveganj se ugotavlja, če so se tveganja spremenila, če je obvladovanje tveganj uspešno oziroma so potrebni dodatni ukrepi za obvladovanje tveganj.



Slika 1: Register tveganj v procesih, na projektih, …

Odgovorni subjekti javne uprave pregledujejo zrelost upravljanja tveganj in naročajo izdelavo analiz skladnosti ISO/IEC 27001. Na podlagi izvedene analize dobi naročnik seznam ugotovljenih odstopanj od zahtev in priporočil standardov ISO/IEC 27001 in ISO/IEC 27002. Na osnovi ugotovitev so oblikovana priporočila za izboljšanje stanja, razdeljena na hitre ukrepe, pomembna priporočila in ostale ukrepe. Ključni elementi vzpostavitve sistema vodenja varovanja informacij v praksi so izdelava analize tveganj, izvedba notranje presoje in izvedba vodstvenega pregleda (Saksida, 2011).



Slika 2: Centralni register tveganj - navodilo za izpolnjevanje obrazca

Za redno posodabljanje registra tveganj imenujejo skrbnika upravljanja s tveganji, ki koordinira aktivnosti pri izpopolnjevanje, skrbi, da so odgovorni seznanjeni s spremembami, ki vplivajo na potrebne dopolnitve registra tveganj. Veliko pozornost nameni spremljanju, če so opredeljena tveganja še vedno relevantna in opredeli nova tveganja, preveri ali so ukrepi za obvladovanje tveganj še vedno primerni in oceni primernost kontrolnih mehanizmov, ki omogočajo vrednotenje upravljanja s tveganji.

Po pripravi pregledne obravnave tveganj vseh procesov oziroma organizacijskih enot in s tem obravnavo groženj za dosego ciljev organizacije, se pristopi še k urejanju ključnih področij organizacije. Ena od prioritetnih v javni upravi je vsekakor vzpostavitve sistema vodenja varovanja informacij. Že dlje časa si ni moč predstavljati sodobne, prijazne in učinkovite javne uprave brez visoke stopnje informatizacije, ki uporabnikom zagotavlja varno delo in izmenjavo podatkov.

Ob vedno večji odvisnosti od informacijskih tehnologij, odprtosti organizacij in povečevanju pomena informacij v sodobnem poslovanju sta iz želje po ureditvi in poenotenju razmer v organizaciji na področju informacijske varnosti, nastala standarda za vodenje varovanja informacij ISO/IEC 27002 in ISO/IEC 27001. Standarda sta poslovodno in od posameznih tehnoloških rešitev neodvisni orodji, ki ponujata celovit pregled varovanja informacij pri poslovanju organizacije. Ocena informacijskih tveganj je osnova za izgradnjo sistema vodenja varovanja informacij in njegova temeljna značilnost (Lemič, 2011).

Velja poudariti poslovne koristi, ki jih dosežemo z vzpostavitvijo sistema vodenja varovanja informacij: prepoznavanje in zmanjšanje varnostnih tveganj na želeno raven, izboljšanje poslovnih partnerstev (večja zaupnost medsebojno izmenjanih informacij), obvladovanje procesov varovanja informacij.

Večji delež organizacij (60%) ugotavlja, da je za njihovo uspešno in nemoteno delovanje kritična zaščita podatkov. Pri tem preseneča dejstvo, da so nekatera podjetja opredelila kot pomembno tudi strojno opremo informacijskega sistema. Z vidika zaščite podatkov in integritete je to vsekakor smiselno, vendar meniva, da je za uspeh organizacije kritična predvsem zaščita podatkov ob jasni predpostavki, da je na delu strojne in programske opreme izvedeno vse, kar zagotavlja stabilen, varen učinkovit in zmogljiv IS.
Pri ocenjevanju pogostosti napadov na informacijski sistem skoraj polovica (45%) organizacij navaja, da so napadi na njihov sistem redki. Četrtina izprašanih trdi, da napadov na sistem sploh nimajo, ostale organizacije pa beležijo pogostejše napade na njihov informacijski sistem. Vendar pa je ocenjevanje pogostosti napadov na informacijski sistem kritično. Podjetja namreč delujejo le na podlagi detektiranih napadov na sistem, ob tem pa mnogokrat pozabljajo, da mnogo napadov na sistem ni detektiranih. Le ti pa pomenijo mnogo večjo grožnjo sistemov z vidika – če ne poznaš problema ga ne odpravljaš (Bernik in Prislan, 2010).

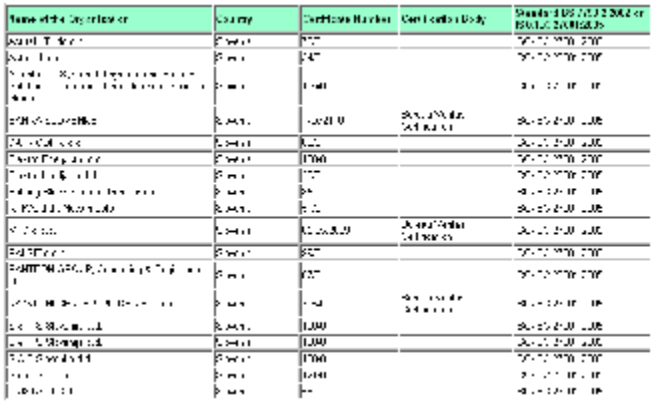
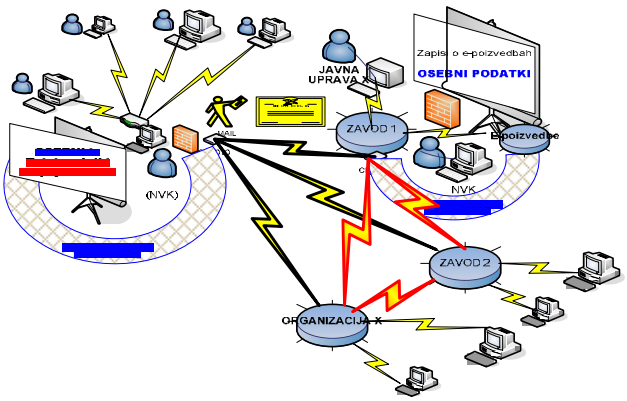


Tabela 3: Seznam organizacij in podjetij, ki so že pridobila certifikat ISO 27001 in ISO 27002
(Register Search, 2011)

Pregled organizacij in podjetij, ki so že pridobila certifikat ISO 27001 in ISO 27002 (Register Search, 2011) pokaže na velike priložnosti za posamezne subjekte javne uprave. Seznam certifikatov v zgornji tabeli ni obsežen. Pot do certifikata ISO/IEC 27001 ni enostavna in poceni. Ocenjujemo, da je prioritetna vzpostavitev dobrih praks informacijske varnosti v institucije in zavode javne uprave, ki so močan integrator podatkovnih baz (z osebnimi, občutljivimi in tudi tajnimi podatki). Neustrezna stopnja varovanja, in s tem zagotavljanja informacijske varnosti, predstavlja (pre)veliko tveganje za varno prihodnost in ščitenje (vitalnih) interesov javne uprave in s tem tudi nacionalne varnosti.
Zagotavljanje informacijske varnosti je logičen korak po sprejetem registru tveganj v organizaciji. Naslednji korak je naročilo izvedbe analize skladnosti s standardom ISO 27001, priprava vrste organizacijskih izvedbenih navodil in izobraževanja zaposlenih.

2.2 Sklepanje pogodb z integratorji baz

Sklepanje pogodb/sporazumov z integratorji baz - med dajalcem in prejemnikom (osebnih, občutljivih in zaupnih ter tajnih) podatkov, ki jih glede na zakonske pristojnosti prejemnik tudi obdeluje in posreduje, je naravnano za vzpostavljanje varnostne verige. V pogodbi/sporazumu določita medsebojne pravice ali/in, da bosta kot stranki v svojem dogovoru, kakorkoli ga že poimenujejo, določili medsebojne pravice ali/in obveznosti. Gre za pogodbo, ki ima pravne učinke, da lahko stranke uveljavljajo svoje pravice in da imajo pravico od druge strani zahtevati, da izpolni svoje obveznosti; v skrajnem primeru tudi po sodni poti.



Slika 4: Varnostna veriga – shema povezav

Prenos rešitev in dobrih praks na tem tehnološko zahtevnem področju bo imel želeni učinek le, če bo izveden na urejen način. To je še toliko pomembneje, če se prenašajo občutljivi podatki oziroma »zaupni« ali celo tajni podatki, ki nastanejo z združevanjem ali povezovanjem podatkov v fazi izmenjav podatkov med posameznimi javnimi institucijami, ki sami po sebi niso zaupni oziroma tajni. Tako združene ali povezane podatke (ali sezname oziroma dokumente) je potrebno zavarovati in vzpostaviti nadzor vpogledov, popravkov ali iznosov le-teh v celotnem življenjskem ciklu podatkov.
Zagovarjamo postopnost, z veliko večjo dinamiko in udejanjanjem pobud za večjo stopnjo medresorskega sodelovanja.

3 VZPOSTAVITEV NOVEGA POSLOVNEGA MODELA JAVNE UPRAVE

V tekmi za ohranjanje gospodarske rasti, izhoda iz krize in razvoja se vrsta držav, multinacionalk in večjih podjetij oprijema bližnjic do inovacij, patentov, poslovnih skrivnosti. Poleg etičnih in drugih hekerjev, se z zbiranjem ekonomskih informacij ukvarjajo bolj ali manj specializirane enote obveščevalnih služb. Poleg ekonomskega vohunjenja gre pogosto za izvajanja postopkov strategije posrednega nastopanja, pri čemer največje tveganje predstavljajo zaposleni v javni upravi, kjer je množica podatkovnih baz, kjer so podatki o naprednih tehnoloških postopkih, inovacijah ipd.
Ker gre v takih in podobnih primerih za najtesneje sodelovanje služb in podjetij, je potrebno na drugi strani poskrbeti za pospešeno zagotavljanje visoke stopnje informacijske varnosti in obvladovanja ostalih tveganj, kar je lažje v okviru dobrega medresorskega sodelovanja, ki naj bo del novega modela so-delovanja javne uprave.

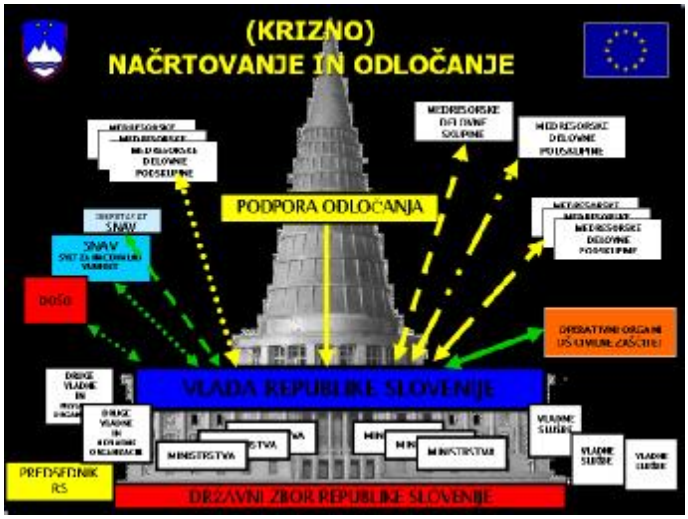
3.1 Izkušnje razvoja, udejanjanja in dopolnjevanja velikega informacijskega sistema

Pri oblikovanju predloga novega modela (medresorskega) sodelovanja za zagotavljanje informacijske varnosti se velja opreti na preizkušene in delujoče prakse in pristope. Dolgoletne izkušnje pri razvoju, udejanjanju in stalnem dopolnjevanju ter nadgradnji sistema MFERAC (računalniška podpora enotnemu računovodstvu RS) so zgled dobre prakse in sinergij medresorskega sodelovanja. Predstavljenih je nekaj tez, ki opredeljujejo pristop in oblike sodelovanja za doseg ciljev javne uprave. Prva teza potrjuje, da je bilo medresorsko sodelovanje ključ uspeha izgradnje vladnega poslovnega - ERP sistema.

Izkušnje in kompetence uporabnika javne uprave A
+ Izkušnje in kompetence uporabnika javne uprave B
+ …
+ Potrebe vodstva (ključnih nosilcev odločanja)
= garancija za sinergijo, večjo učinkovitost in uspešnost udejanjanje poslovnega obveščanje ter **zagotavljanje informacijske varnosti v javni upravi**

Slika 5: Pot do učinkovitejše in uspešne informacijske varnosti v javni upravi (Cvelbar, Sladoje in Savernik, 2006)

Predstavljena teza, zgled dobre prakse, predstavlja eno od poti za zagotavljanje višje stopnje informacijske varnosti v javni upravi in širše. Prizadevamo si, da bi bilo še večkrat uporabljeno temeljno vodilo, uporabljeno na vrsti velikih (medresorskih) projektov, oblikovano v predstavljeni tezi.
Dopolnjevan sistem MFERAC in integracija z vrsto drugih aplikacij predstavlja osrednje, učinkovito in več kot deset let delujoče informacijsko orodje poslovnega obveščanja v državni upravi. S tem v zvezi bo potrjena druga teza o potrebi odločevalcev po učinkovitem orodju za podporo odločanja.



Slika 6: Več integracije za celovitejše poslovno obveščanje in krizno upravljanje (Cvelbar, Mlinar in Cvar, 2008)

3.2 Kriza in realističen pogled

Kriza in vrsta groženj ter tveganj je priložnost za prestrukturiranje, za nove produkte, prenovo podjetij in organizacij ter tudi javne uprave. Krize so nekaj običajnega; pridejo vsakih 10 let. Posledice so večje v bolj razvitem svetu. Kriza kot priložnost za prečiščenje –»katarzo«. Nizanje dejstev o vsepovsod prisotni krizi, težave kot posledice slabih praks in negiranja stanja v katerem smo ter slabe napovedi, stečaji in bankroti so dejstva; prihodnost vrsto let ne bo več cvetoča, velika gospodarska rast je do nadaljnjega preteklost (Damjan, 2010).
Za prepoznavanje lastnosti in (vse)obsežnosti kriz je poučna seznanitev z študijama: *Reinhart* and *Rogoff* (2008)*: This Time is Different: A Panoramic View of Eight Centuries of Financial Crises (Reinhart, 2008). Obsežnejše, temeljito in slikovito gradivo ponuja "panoramsko" analizo zgodovine finančnih kriz od štirinajstega stoletja do sedanje krize (od Angleške krize vse do globalne finančne krize, ki je nastala v ZDA). Drugo gradivo je: Carmen M. Reinhart, Kenneth S. Rogoff: The Aftermath of Financial Crises (Reinhart, 2009).

Med poraženci krize (kriz) je vrsta podjetij in organizacij, ki je uporabljala naprednejša orodja za podporo odločanja in BI. Več pozornosti naj zatorej velja vsebinam, ki so plod izkušenj (dobrih in slabih praks) pri oblikovanju, izgradnji, udejanjanju ter uvajanju podpore za odločanje in nadzor nad delovanjem/izvajanjem temeljnih in podpornih procesov. Izkušnje in poznavanje teoretičnih primerov nam razkrijejo vrsto pasti in temu prilagojenih pristopov, ki jih je potrebno izvajati pri uporabi najenostavnejše podpore odločanja, kot tudi pri delu z »naprednimi« orodji BI. Na konferenci SIOUG 2011 so bila predstavljena tista navodila, priporočila in opozorila ključnim strokovnjakom in managerjem, ki bi morala biti navedena v drobnem tisku z velikimi črkami v vseh fazah poslovanja in uporabe BI-ja (Cvelbar, 2011).
So posamezne rešitve res rešitev? Ne! Potrebne so celovite rešitve, s kar najbolj ažurnim pregledom tveganj, uporabo učinkovitih orodij poslovnega obveščanja. Za zanesljivo in varno delovanje je potrebno zagotavljati visok nivo informacijske varnosti.

3.3 Poslovni obveščevalni sistemi - poslovna inteligenca

Za uspešno prilagajanje spreminjajočemu zunanjemu okolju morajo podjetja in organizacije razviti sposobnosti simuliranja potencialnih razvojnih poti in s tem povezanih tveganj. Dejavnosti vse bolj temeljijo na naprednih rešitvah poslovnega obveščanja (BI) s širokim spektrom tehnoloških orodij za "pametna podjetja".
Kako izkoristiti poslovni potencial BI sistemov nove generacije? Organizacije, ki uporabljajo BI, vedo več od ostalih in so bolj uspešne. Zakaj potem nimajo vse organizacije razvitega BI? Nekaj razlogov: dragi in dolgotrajni projekti, pomanjkanje podpore implementaciji, nezadovoljstvo uporabnikov in nenazadnje več kot 50% projektov ne prinese pričakovanih koristi. Tradicionalni BI poudarja tehnični vidik dostave informacij, poenostavlja poslovno realnost in poudarja tehnično kompleksnost. Analitične potrebe je možno vnaprej definirati, za rešitev naših težav moramo zgraditi podatkovno skladišče, saj javna uprava postaja „vesolje podatkov“.
Naprednejši BI je v osnovi poslovni projekt in ne tehnološki, kjer pridobimo na času uvajanja, enostavnosti in zagotavljamo podporo spreminjajočim ciljem. Zmogljivost poslovnih sistemov kombinira z izkušnjo iz različnih aplikacij, zagotavlja izredno enostavno uporabo, zagotavlja ponazoritev zapletenih stvari na enostaven način, skrbi za konsolidacijo poljubnih virov, obljublja hitre rezultate in olajša odgovore na nepredvidena vprašanja.
Informacijska varnost podpira tudi pomembno blago javne uprave - arhiviranje podatkov, kjer je potrebno zagotavljati neprekinjen, varen in hiter dostop do poslovnih podatkov in aplikacij vedno in vsepovsod. Zaščita za veliko število strežnikov, prenosnikov ali delovnih postaj ob hitri obnovitvi podatkov in takojšen prenos na varno oddaljeno lokacijo. Javna uprava ima na množici lokacij ogromno količino dokumentov, katere je treba skrbno hraniti. Ena glavnih skrbi je kakovostna zaščita svojih in vsem njim zaupanih dokumente, saj le tako lahko varno in nemoteno posluje. Navedeno, glede na visoko stopnjo digitalicacije zahteva zagotavljanje varnostnih kopij podatkov, skrbno varovanje in kakovostno zaščito podatkov. Arhiviranje podatkov zajema tudi (nedokončane) analize in študije, predvidevanja (scenarije) in druga delovna gradiva ter zapise.

3.4 Moč povratnih informacij in varnostna kultura

Visok nivo varnostne kulture v posamezni službi oziroma organizaciji prispeva k bistveno manj priložnostim za različne manipulacije in zlorabe. Sodelovanje vseh zaposlenih v organizaciji prispeva k izgradnji in vzdrževanju stabilnega in varnega delovnega okolja. Tako ali drugače so za varnost v organizacijo odgovorni vsi njeni člani in širše tudi pogodbeni in medresorski partneji oz. sodelavci.
Opazen je napredek. Ministrstvo za javno upravo je oktobra in novembra 2011 izvajalo prvi del varnostnega pregleda. Pri nekaterih ukrepih bi s centralnim upravljanjem informacijske varnosti ali s standardizacijo rešitev (kot horizontalna funkcija) lahko dosegli velik odstotetk zaščite pred vdori in škodljivo programsko kodo (Marinšek, 2011).

Nezadostna stopnja zaščite je vzrok in povod vsem nerazumevanjem in napačnim predstavam o resnosti in nevarnosti sodobnih groženj informacijskim sistemom. Največ kar lahko organizacije na

tem mestu naredijo takoj, je izobraževanje in ozaveščanje zaposlenih ter uporabnikov informacijskega sistema. S tem se dviga stopnja varnostne kulture in tudi dejanska stopnja informacijske varnosti (Bernik in Prislan, 2010). Velika tveganja nastopijo, ko pride do incidenta in se o tem ne obvesti vseh odgovornih, vključno z osebjem in institucijami, katerih podatki so bili razkriti ali odtujeni.

3.5 Novi model so-delovanja javne uprave

Odzivanje na krizo zahteva medresorsko združevanje. Dobre prakse in izkušnje bi morali vključiti v koordinacijsko telo, čemur bi sledilo modularno oblikovanje koordinacij. Gospodarska kriza je tudi priložnost, da poskrbimo za notranje ravnovesje poslovanja, obdržimo tržno uveljavljene storitve in produkte z boljšo dodano vrednostjo ter optimiziramo poslovne procese. Zato moramo poslovne procese dobro poznati. Katera področja poslovanja so ključna in zahtevajo največ pozornosti? »Slovenska gospodarska struktura izpred zadnje krize je preživeta, zato so težave večje. Spremembe zahtevajo vključevanje novih poslovnih modelov (Damjan, 2010).
SREP je oblikovan in potrjen pristop za uravnotežen razvoj elektronskega poslovanja v javni upravi in prenos rešitev ter dobrih praks, ki so nastale na področju e-uprave, na druga področja elektronskega poslovanja v javni upravi. Na področju strateških ciljev SREP-a so navedeni tudi cilji, ki se nanašajo na varnost poslovanja javne uprave, varstvo osebnih podatkov in zanesljivost in razpoložljivost delovanja informacijskih sistemov. S tem v zvezi se kaže potreba, da resorno ministrstvo zagotovi in koordinira več podpore vsem tistim državnim organom in javnim institucijam, ki jih posebej skrbi obvladovanje, varovanje in zaščita občutljivih in zaupnih podatkov, ki nastanejo z združevanjem.
Državni organi in javne institucije, ki se zavedajo vse večje vrednosti baz podatkov, ki nastaja s porastom elektronskega poslovanja in vse večjim številom združenih (iz več različnih naslovov pridobljenih ali izmenjanih podatkov) podatkovnih baz, opozarjajo na varnostna tveganja. Gre za občutljivost celotne varnostne verige, v kateri pride lahko do posrednih odtekanj občutljivih podatkov iz podatkovnih baz. Le-te so lahko »daleč« od institucije, ki je, v skladu z zakonom posredovala podatke. Tveganja za dajalce podatkov se povečajo z združevanjem ali povezavo z drugimi podatki.
Nadzorne plošče so primerne, ko potrebujemo hiter pregled nad raznovrstnimi informacija, ki bi lahko vplivale na poslovanje podjetja. Na plošči so združene informacije iz različnih virov, ki našo pozornost usmerijo k pomembnim področjem. Uporaba nadzornih plošč prihrani čas, ki bi ga porabili za pregled posameznih poročil, ter prepreči, da bi prezrli katero od področij, ki zahtevajo naš poseg (Perko, 2011).
Tretja teza predstavlja izziv in priložnost oblikovanja registra tveganj v funkciji nadzorne plošče upravljanja informacijske varnosti. V primeru oblikovanih in ažurno dopolnjevanih (centralnih) registrov tveganj lahko na nadzorni plošči z enega mesta spremljamo informacije o upravljanju:

- na treh ravneh: grafične elemente, ključne vrednosti in povezave do analitičnih in drugih poročil, analiz ter dokumentov;
- na več nivojih, ko imamo »pod« centralnim registrom še vrsto spodnjih nivojev (registre tveganj v procesih, na projektih ali področjih oziroma sistemih kot je npr. upravljanje informacijske varnosti.

Nov model so-delovanja javne uprave bi se lahko udejanjil prek sveta za informacijsko varnost kot stalno koordinacijo za pospešeno oblikovanje minimalnih in višjih standardov za varovanje osebnih in drugih občutljivih podatkov. Naša dokumentirana pričakovanja so se deloma uresničila s sprejetjem IVJPU. Znatne napore bi morali prek novega modela so-delovanja javne uprave usmeriti v implementacijo standardov družine ISO 27000 ali nekatere elemente le-teh. Prioriteta velja implementaciji elementov teh standardov v tista okolja javne uprave, kjer gre za izmenjave občutljivih podatkov iz uradnih evidenc. Pričakovanja so podprta z dejstvom, da je javna uprava prepletena z uporabo portala e-VEM, e-Uprava in elektronskega poslovanja pri uporabi posameznih storitev. Posredovanja osebnih podatkov na zunanje institucije in zavode so vplivala na oblikovanje močne integracije podatkovnih baz na ZZZS, ZPIZ, DURS, UJP, AJPES in SURS. Strategija IVJPU omogoča koordiniran pristop k upravljanju varnosti na področju elektronskega poslovanja. Podana je možnost za celovit nadzor nad investicijami na tem področju, zato je pričakovati znatne prihranke v primerjavi z razvojem brez strateškega upravljanja.

4 ZAKLJUČEK

Pozornost oblikovalcev rešitev in odločevalcev velja ažurnemu odzivanju na probleme in pasti. Navedeno zahteva ustrezno informacijsko-telekomunikacijsko opremo in zagotavljanje informacijske varnosti. Mnogi državni organi in javne institucije se zavedajo ranljivosti, in s tem povezanih tveganj, baz podatkov, ki so nastale s porastom elektronskega poslovanja in vse večjim številom združenih podatkovnih baz. Gre za občutljivost celotne varnostne verige, v kateri pride lahko do posrednih odtekanj občutljivih podatkov. Opozorilom za vse večja varnostna tveganja morajo slediti odločnejši ukrepi.

Prenos rešitev in dobrih praks na tem tehnološko zahtevnem področju bo imel želeni učinek le, če bo izveden na urejen način. To je še pomembneje, če se prenašajo občutljivi ali tajni podatki. Posebne težave povzroča varovanje tajnih podatkov, ki nastanejo z združevanjem ali povezovanjem podatkov v fazi izmenjav podatkov med posameznimi javnimi institucijami, ki sami po sebi niso zaupni oziroma tajni. Tako združene ali povezane podatke je potrebno zavarovati in vzpostaviti nadzor vpogledov, popravkov ali iznosov le-teh v celotnem življenjskem ciklu podatkov.

Modularni pristop, ki je cenovno sprejemljiv, pomeni prilagajanje sheme/modela upravljanja varnostnih tveganj in racionalizacija delovanja s krajšimi odzivnimi časi ter celovitim pregledom, ki presega delovanje posameznih, premalo ažurnih medresorskih delovnih skupin. Kjer ni celovitosti, zmanjka priložnosti za sinergijo in kreativnost. Po drugi strani modularni pristop in interdisciplinarno delovanje omogoča veliko odzivnost, kar državi omogoči, da smo med prvimi na kriznem področju in ob tem ažurno spremljamo situacijo širše in celoviteje. Žal smo na vrsti področij izgubili dinamiko. Naj bo prispevek izziv za pozitivno naravnanost in odločnejše delovanje usklajenih ekip.

Centralni register tveganj, kot nadzorna plošča upravljanja informacijske varnosti javne uprave, je lahko učinkovita podpora odločevalcem za zaustavitev nazadovanja in podpora na poti iz krize.

VIRI

Berk, A., Peterlin,J. in Ribarič,P. (2005). Obvladovanje tveganja, Ljubljana: GV Založba

Bernik,I. in Prislan, K. (2010). Proces upravljanja s tveganji v informacijski varnosti. Fakulteta za varnostne vede, Univerza v Mariboru

Cvelbar,B., Sladoje,J.A. in Savernik,D. (SIOUG 2006). Poslovno obveščanje v javni upravi v okviru medresorskega sodelovanja, Konferenca SIOUG, Portorož

Cvelbar,B., Mlinar,J. in Cvar,B. (2008). Več integracije za celovitejše poslovno obveščanje in krizno upravljanje, Konferenca SIOUG, Portorož

Cvelbar,B. (2011). Katera BI orodja nam bodo v pomoč in kaj bo potrebno spremeniti za izhod iz krize? Konferenca SIOUG, Portorož

Damijan,J.P. (2010). Finančna kriza ter smeri izhoda iz krize, pomen regulacije in novih poslovnih modelov podjetij, 5. konferenca »Best BI Event in Town« , Ljubljana

Lemič,J. (2011) ISO/IEC 27001:2005 sistemi vodenja varovanja informacij. Pridobljeno 14.12.2011, na http://www.siq.si/ocenjevanje_sistemov_vodenja/storitve/sistemi_vodenja_varovanja_informacij/index.html

Marinšek,D. (2011). Informacijska varnost – informacijska varnostna politika in varnostni pregled, Informatika v javni upravi 2011, Brdo pri Kranju

Perko,I. (2011). Poslovni obveščevalni sistemi-Primeri slovenskih podjetij, Ljubljana: GV Založba

Priporočila informacijske varnostne politike javne uprave. Pridobljeno 13.12.2011, na http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/DEUP/IVPJU.doc_01.pdf

Register Search (Version 211 November 2011) click on a letter to see the certificates. Pridobljeno 14.12.2011, na http://www.iso27001certificates.com/Taxonomy/CertificatesResults.asp

Reinhart,C.M. in Rogoff,K.S. (2008). This Time is Different: A Panoramic View of Eight Centuries of Financial Crises, dostopno na spletni strani: http://www.economics.harvard.edu/files/faculty/51_This_Time_Is_Different.pdf

Reinhart,C.M. in Rogoff,K.S. (2009). The Aftermath of Financial Crises, NBER Program(s). IFM, dostopno na spletni strani: http://www.nber.org/papers/w14656

Saksida, M. (2011). Kako uspešno uvesti informacijsko varnost in pridobiti certifikat ISO/IEC 27001, dostopno na spletni strani: http://znanje.snt.si/tecaji/d9-kako-uspesno-uvesti-informacijsko-varnost.shtml

Strategija razvoja elektronskega poslovanja ter izmenjave podatkov iz uradnih evidenc – SREP. Pridobljeno 13.12.2011, na http://zakonodaja.gov.si/rpsi/r04/predpis_STRA54.html

---

Prispevek izraža stališče avtorja in ne nujno tudi organizacije, v kateri je zaposlen.