ANALIZA TVEGANJA ELEKTRONSKEGA POSLOVANJA MED GEODETSKO UPRAVO REPUBLIKE SLOVENIJE IN GEODETSKIMI PODJETJI

RISK ANALYSIS OF ELECTRONIC COMMERCE BETWEEN THE MAPPING AND SURVEYING AUTHORITY OF THE REPUBLIC OF SLOVENIA AND SURVEYING COMPANIES

Franc Ravnihar

UDK: 004:061.5:35:528

POVZETEK

Prispevek obravnava manjši segment področja varnosti elektronskega poslovanja. V prispevku je na osnovi evidentiranih dobrin in možnih groženj ter ob oceni ranljivosti dobrin ocenjen nivo tveganja v okviru informacijske varnosti na področju poslovanja med geodetsko upravo in geodetskimi podjetji. Najpomembnejša zaključna ugotovitev je, da zagotavljanje varnosti na področju elektronskega poslovanja ni enkratno opravilo, ampak je to proces stalnega spremljanja predvidenih aktivnosti, izobraževanja in uvajanja novosti, ki jih omogočajo nove tehnologije in nova spoznanja.

KLJUČNE BESEDE

elektronsko poslovanje geodetske uprave, varnost, analiza tveganja

Klasifikacija prispevka po COBISS-u: 1.04

ABSTRACT

The article deals with a minor topic from the electronic commerce security sphere. An estimation of the level of risk of information security commerce between the Surveying and Mapping Authority and surveying companies is represented, based on the recording of goods, possible threats and estimation of vulnerability of goods. The most important final conclusion is that assuring security of electronic commerce is not a unique occurrence, but first of all a process of permanent monitoring of activities, education and introduction of new technologies.

KEY WORDS

electronic commerce of the Surveying and Mapping Authority, security, risk analysis

1 UVOD

Geodetska uprava Republike Slovenije (v nadaljevanju: geodetska uprava) je državni organ – organ v sestavi Ministrstva za okolje in prostor in kot taka del javne uprave. Ta nedvomno sodi med največje upravljavce zbirk podatkov, kar velja tako glede različnih sektorjev kot tudi nivojev (državni, regionalni, lokalni). Podatki javne uprave so izredno pomembni pri delovanje trga, prosti izmenjavi dobrin, storitev in ljudi (Evropska komisija, 1999). Javnost delovanja javne uprave in pravica dostopa do podatkov in informacij javne uprave je splošno sprejeto načelo v sleherni moderni demokratični družbi. To je hkrati tudi pogoj za normalno delovanje javne uprave, ki brez zaupanja, sodelovanja in podpore javnosti praktično ne more biti učinkovita.

Naloge in dela, ki jih izvaja geodetska uprava, so predpisani z zakoni in drugimi predpisi. Med pomembnejše naloge sodijo naloge s področja vodenja in vzdrževanja evidenc: zemljiškega katastra, katastra stavb, evidence hišnih številk, registra prostorskih enot ... V okviru celotnega postopka, ki pripelje do sprememb podatkov v uradnih evidencah, so poleg geodetske uprave

udeležena tudi geodetska podjetja, ki za tovrstne dejavnosti izpolnjujejo določene pogoje in so pridobila ustrezna dovoljena. Pri tem sodelovanju in povezovanju med geodetsko upravo in geodetskimi podjetji prihaja do velikega pretoka podatkov, in sicer v obeh straneh. V eni smeri gredo podatki iz obstoječih evidenc in aktivnega arhiva, na drugi strani se vračajo podatki o novem stanju na terenu. Od pravilnosti in celovitosti podatkov je odvisna pravilnost in kvaliteta geodetske storitve in končnega stanja v uradnih evidencah. Posledica tega je zagotavljanje kakovostne in vsebinsko pravilne baze podatkov, ki so na voljo vsem uporabnikom.

Ker bi celovita analiza vseh dobrin, groženj in tveganj, ki veljajo za celoten informacijski sistem geodetske uprave, bistveno presegala okvir tega prispevka, je vsebina omejena samo na vidik poslovanja geodetske uprave z geodetskimi podjetji. Brez velikega tveganja pa velja ocena, da podobne ugotovitve veljajo za celotno področje poslovanja geodetske uprave kakor tudi za geodetska podjetja, ki sodelujejo z geodetsko upravo.

2 OCENA STANJA

Organi javne uprave praviloma skrbijo za svojo informacijsko varnost. Pri tem v večji ali manjši meri upoštevajo ustrezna priporočila Centra Vlade RS za informatiko (v nadaljevanju: CVI). To upoštevanje je odvisno od več faktorjev – zainteresiranosti posameznega organa, njegovih kadrovskih in finančnih možnosti pa tudi od obsega in nivoja elektronskega poslovanja.

Splošna ugotovitev za geodetsko upravo bi lahko bila, da v sodelovanju s CVI in v okviru predpisov (Pravilnik, 2002) dokaj solidno skrbi za varnost svojih podatkov, za varno in zanesljivo delovanje vseh sistemov. Kljub temu je zaslediti pomanjkanje celovite informacijske varnostne politike, ki bi vodstvu, vsem zaposlenim in tudi zunanjim sodelavcem služila kot neposreden vir pravil in navodil za učinkovito in varno uporabo informacijsko-telekomunikacijske opreme in varovanje podatkov. Vsi ti elementi so sicer po posameznih segmentih zajeti v raznih navodilih, priporočilih, okrožnicah, vendar so bolj odraz in rezultat trenutnih potreb in zahtev kot pa celovitega sistema varovanja. Zaradi navedenega bi bilo treba vzpostaviti stalni postopek zagotavljanja in vzdrževanja informacijske varnosti. Ta se praviloma začne z analizo in oceno vseh tveganj, ki izhajajo iz obdelave podatkov in uporabe sodobne informacijsko-telekomunikacijske tehnologije in kasneje nadaljuje z zasnovo ukrepov za zmanjševanje ugotovljenih tveganj in pripravo jasnih pravil in navodil, s katerimi se zagotovi informacijska varnost (Hajtnik, 2002).

3 OPREDELITEV OSNOVNIH POJMOV

V literaturi lahko najdemo več definicij pojmov, ki so tako ali drugače povezani z varnostjo in varovanjem informacijskih sistemov. Za boljše razumevanje vsebine prispevka bodo uporabljeni in opredeljeni naslednji pojmi:

3.1 Varnost

Je sposobnost sistema, da pri določenih pogojih opravlja predvidene funkcije brez pojavov in dogodkov, nastalih bodisi naključno bodisi zaradi namerne ali nenamerne človekove dejavnosti, ki bi lahko porušili njegovo normalno in celovito delovanje (Hudoklin in Šmitek, 1991).

3.2 Dobrine

Dobrine so osnovni sestavni deli opazovanega sistema, ki jih želimo varovati. Predstavljajo lahko katero koli stvar, ki je pomembna za nemoteno delovanje sistema. Ko govorimo o varnosti neke dobrine, moramo v prvi vrsti identificirati, katere dobrine želimo varovati in določiti njihove vrednosti. Vrednost lahko izražamo v denarnih enotah, lahko pa uporabljamo opisne mere (zelo pomembna, pomembna, manj pomembna) (Šmitek, 1992).

Dobrine lahko razdelimo na več skupin. V okviru prispevka bodo obravnavane le nekatere iz sklopa nujno potrebnih dobrin (označeno odebeljeno), ki so definirane v skladu s standardom BS 7799:

- ljudje
- **strojna oprema (računalniki, periferna oprema)**
- **programska oprema**
- **komunikacijska oprema**
- zgradba (prostori)
- energija
- mrežne naprave
- instalacije
- **podatki (datoteke, baze podatkov)**

3.3 Grožnje (P)

Varnost računalniško podprtega informacijskega sistema je zaradi njegove občutljivosti in ranljivosti ves čas pod pritiskom groženj. Grožnje se porajajo znotraj sistema samega in v okolju sistema (Hudoklin in Šmitek, 1991). So specifični dogodki ali aktivnosti, ki povzročajo motnje v delovanju sistema ali posamezne dobrine. V grobem jih lahko razdelimo na:

- izredne dogodke (naravne katastrofe): poplave, potres, požar, strela,
- odpovedi delovanja: elektrike, telefonskih in drugih ITk-zvez, strojne opreme, programske opreme, ogrevanja oz. hlajenja,
- namerne človekove dejavnosti: kraja, vlom, sabotaža, izsiljevanje, vandalizem,
- nenamerne človekove dejavnosti: napake osebja, napačno vodenje ...

Grožnje po posameznih elementih je v praksi težko ocenjevati kvantitativno, zato bodo v nadaljevanju ocenjene vrednostno – v obliki pogostosti oz. verjetnosti nastopa posamezne grožnje, npr. pogosto, občasno, manj pogosto, in opisno – v obliki mer kot zelo verjetno, verjetno, malo verjetno.

3.4 Ranljivost (C)

Predstavlja pomanjkljivost sredstev oz. stroške, ki s tem nastanejo. Od stopnje ranljivosti je odvisno, kako velik vpliv bo imela grožnja na posamezno dobrino. Ta bo tem večji, čim slabše je neka dobrina zaščitena zoper grožnjo.

3.5 Tveganje (R)

Je kombinacija pogostosti groženj posamezne dobrine in njene ranljivosti, ki se odraža skozi verjetnost grožnje in skozi stroške, ki pri tem nastanejo. Lahko jo izrazimo s formulo: R = P * C.

3.6 Analiza tveganja

Je postopek na podlagi katerega iz izbranih kombinacij in medsebojnih odvisnosti dobrin, groženj in ranljivosti izberemo in evidentiramo tiste, ki so pomembne oziroma imajo večji vpliv na delovanje informacijskega sistema.

4 OPIS INFORMACIJSKEGA SISTEMA GEODETSKE UPRAVE

Kot je že navedeno-, je v prispevku obdelan le manjši del celotnega informacijskega sistema geodetske uprave, in sicer tisti del, ki zagotavlja nemoteno poslovanje geodetske uprave na področju izmenjave oziroma pretoka podatkov z geodetskimi podjetji. Zaradi lažje predstave, predvsem pa lažjega dostopa do potrebnih podatkov oz. informacij, ki so bile potrebne za izdelavo analize, je bila le ta opravljena v okviru ene organizacijske enote – Območne geodetske uprave Kranj (lokacija Kranj). Brez velikega tveganja lahko ugotovimo, da bi bilo možno rezultate upoštevati in ekstrapolirati na vse organizacijske enote geodetske uprave.

V konkretnem primeru je obravnavan informacijski sistem, ki zagotavlja vodenje in vzdrževanje podatkov zemljiškega katastra. Ta sistem vključuje in podpira tako osnovne funkcije vodenja postopkov kot tudi vse postopke v zvezi s izdajanjem podatkov, potrebnim obračunavanjem, vodenjem statistike, arhiviranjem. Posledično zgodovinskemu nastanku ter današnji organiziranosti poslovanja geodetske uprave informacijski sistem trenutno še deluje v okviru lokalnih rešitev, čeprav vzporedno tečejo tudi že posamezne rešitve na nivoju centralne baze podatkov, v teku pa so tudi projekti, ki bi v celoti zagotavljali poslovanje na nivoju centralnih baz podatkov.

5 ANALIZA TVEGANJ

Predmet analize je sistem (podsistem) za posredovanje oz. izmenjavo podatkov med geodetsko upravo in geodetskimi podjetji. Pri tem sta zajeti oz. obravnavani obe možni varianti poslovanja med geodetsko upravo in geodetskim podjetjem, in sicer posreden in neposreden dostop do podatkov. Posreden dostop do podatkov pomeni najprej zahtevo geodetskega podjetja, pripravo ustreznih podatkov na strani geodetske uprave in distribucijo teh podatkov do geodetskega podjetja. Možnih je več variant posredovanja zahtev in distribucije podatkov: fizični prenos, prenos preko medija (disketa, CD) ali pa prenos preko omrežja (elektronska pošta).

Cilj analize ni bil zajeti vse elemente, pač pa le tiste najpomembnejše, ki imajo tudi največji vpliv na rezultate poslovanja.

5.1 Določitev ocen elementov analize tveganja

Ocena elementov analize tveganja zajema:

- definiranje dobrin sistema,
- oceno stopenj groženj (pogostost grožnje),
- oceno stopenj ranljivosti (velikost stroškov),
- oceno stopenj tveganja.

5.2 Dobrine sistema

5.2.1 Strojna (fizična) oprema

- lokalni strežnik (lokalni – OGU Kranj, lokacija Kranj),
- spletni strežnik za zagotavljanje povezave z internetom in elektronsko pošto,
- UPS-napajalnik,
- 25 delovnih postaj (osebni računalniki),
- UTP-omrežje (kabli),
- 6 mrežnih in več lokalnih tiskalnikov.

5.2.2 Programska oprema

- omrežna programska oprema (Novell 5.0),
- programska oprema za arhiviranje podatkov na strežniku (ArcServe 6.0),
- operacijski sistem na delovnih postajah (osebnih računalnikih) – Windows 2000 oz. Windows NT,
- programska oprema za zaščito pred virusi – Sophos,
- niz internih aplikacij, ki zagotavljajo vodenje in vzdrževanje geodetskih podatkov (DEVO, EVELA, ZK TOC, ARHIV, EDIT_DKN, GEOSS).

5.2.3 Komunikacijska oprema

- spletni vmesnik – e-portal oz. spletna aplikacija za dostop geodetskih podjetij do podatkov (PREG),
- omrežje HKOM (hitro komunikacijsko omrežje državnih organov).

5.2.4 Podatki

- baze podatkov zemljiškega katastra (pisni in grafični podatki o parcelah, lastnikih, zemljiškokatastrskih točkah, arhivski podatki, delovodniški podatki) in podatki ostalih povezanih evidenc (podatki o stavbah in delih stavb, topografski podatki, geodetske točke, podatki registra prostorskih enot ...),
- »baza« datotek, ki jo tvorijo standardizirani obrazci, potrdila, naročila, poročila, računi.

5.3 Ocena stopenj groženj (pogostost – verjetnost grožnje – P)

Ocena stopenj groženj je izvedena opisno po posebni lestvici, kjer je stopnja grožnje odvisna od

pogostosti posameznega pojava, kar je razvidno iz preglednice 1. Definiranje stopenj in razpon sta narejena na osnovi lastnih izkušenj in pridobljenih podatkov s strani sodelavcev, zadolženih za področje informatike na geodetski upravi.

STOPNJA	POGOSTOST GROŽNJE	KRATKA OZNAKA
visoka	do 1-krat na mesec	**V**
srednja	do 3-krat na leto	**S**
nizka	do 1-krat na leto	**N**
zelo nizka	do 1-krat na več let (5 in več let)	**ZN**

Preglednica 1: *Ocena stopenj groženj (pogostost groženj).*

5.4 Ocena stopenj ranljivosti (stroški – C)

Tudi ocena stopenj ranljivosti oz. stroškov je izvedena opisno po posebni lestvici, kjer je glede na posamezno stopnjo ocenjena okvirna finančna vrednost stroškov, ki lahko nastanejo pri posamezni stopnji. Finančna ocena je izvedena na osnovi ocene stroškov za posamezna dejanja, ki jih je treba opraviti za sanacijo. Pri tem ni nujno, da se zaradi posledice posamezne grožnje izvedejo vsa možna dela. Opis je razviden iz preglednice 2. Pri teh ocenah so v glavnem upoštevani stroški porabljenega časa in materiala, da se odpravi posledice groženj. Tudi v tem primeru so bili v pomoč ocene in podatki sodelavcev informatikov.

STOPNJA	OCENJENA VREDNSOT V SIT	KRATKA OZNAKA	OPIS MOŽNIH DEL (glej spodaj)
velika	več kot 1 000 000	**V**	**(1)**
srednja	od 50 000 do 1 000 000	**S**	**(2)**
nizka	do 50 000	**N**	**(3)**

Preglednica 2*: Ocena stopenj ranljivosti (stroškov).*

(1) zamenjava strežnika, nova vzpostavitev baz, nova instalacija programske opreme, zamenjava komunikacijske opreme (omrežje),

(2) ponoven zagon strežnika, restavracija in indeksiranje baz, zamenjava diskov, zamenjava posameznega osebnega računalnika ali UPS-napajalnika, ponovno definiranje uporabnikov in gesel ...,

(3) ponoven zagon sistema (strežnika ali osebnega računalnika), kontrola delovanja, kopiranje in zaščita diskov.

5.5 Ocena stopenj tveganj – R

Ocena stopenj tveganj je opredeljena z upoštevanjem lestvice stopenj iz preglednice 3, kjer so definirane stopnje tveganja v odvisnosti od pogostosti posamezne grožnje in velikosti stroškov, ki lahko nastanejo pri tem. Glede na kvalitativno stopnjo tveganja iz preglednice 4 so na koncu prispevka tudi predlagani potrebni ukrepi.

P \ C	V x > 1 000 000 (SIT)	S 1 000 000 ≥ x ≥ 50 000 (SIT)	N x < 50 000 (SIT)
V (mesečno)	**1**	**2**	**3**
S (3-krat letno)	**1**	**3**	**5**
N (letno)	**2**	**4**	**6**
ZN (večkrat letno)	**4**	**5**	**6**

Preglednica 3: *Ocena stopenj tveganj.*

Stopnja ocene tveganja	Kvalitativen opis tveganja
1	izredno veliko
2	veliko
3, 4	povprečno
5, 6	majhno

Preglednica 4: *Kvalitativna ocena stopenj tveganj.*

5.6 Soodvisnost elementov analize po vrstah dobrin in glede na vrste groženj

Iz naslednjih preglednic so razvidne soodvisnosti elementov analize posameznih dobrin glede na vrsto grožnje. Po vrsti so bile predmet analize naslednje dobrine: strojna oprema, programska oprema, komunikacijska oprema, podatki.

GROŽNJA	STOPNJA GROŽNJE POGOSTOST (P)	STOPNJA RANLJIVOST STROŠKI (C)	TVEGANJE (vrednost iz preglednice 3)
Naravna katastrofa *(potres, poplava, požar ...)*	**ZN**	**V**	**4**
Odpoved delovanja *(izpad elektrike, prekinitev komunikacij HKOM, izpad delovanja lokalnega omrežja)*	**N**	**S**	**4**
Namerna človekova dejavnost *(diverzija, sabotaža, stavka, kraja)*	**ZN**	**V**	**4**
Nenamerna človekova dejavnost *(napaka, površnost – neizkušenost posameznika, napačna navodila)*	**N**	**S**	**4**

Preglednica 5: *Strojna oprema.*

GROŽNJA	STOPNJA GROŽNJE POGOSTOST (P)	STOPNJA RANLJIVOST STROŠKI (C)	TVEGANJE (vrednost iz preglednice 3)
Naravna katastrofa *(potres, poplava, požar ...)*	**ZN**	**S**	**5**
Odpoved delovanja *(izpad elektrike, prekinitev komunikacij HKOM, izpad delovanja lokalnega omrežja)*	**N**	**N**	**6**
Oteženo delovanje *(virusi, zloraba)*	**S**	**S**	**3**
Namerna človekova dejavnost *(diverzija, sabotaža, stavka, kraja)*	**ZN**	**V**	**4**
Nenamerna človekova dejavnost *(napaka, površnost – neizkušenost posameznika, napačna navodila)*	**S**	**N**	**5**

Preglednica 6: *Programska oprema.*

GROŽNJA	STOPNJA GROŽNJE POGOSTOST (P)	STOPNJA RANLJIVOST STROŠKI (C)	TVEGANJE (vrednost iz tabele 3)
Naravna katastrofa *(potres, poplava, požar ...)*	**ZN**	**S**	**5**
Odpoved delovanja *(izpad elektrike, izpad delovanja lokalnega omrežja, onemogočen dostop)*	**N**	**S**	**4**
Oteženo delovanje *(upočasnitev delovanja HKOM, slabša propustnost, zloraba)*	**S**	**S**	**3**
Namerna človekova dejavnost *(diverzija, sabotaža, stavka, kraja)*	**ZN**	**V**	**4**
Nenamerna človekova dejavnost *(napaka, površnost – neizkušenost posameznika, napačna navodila)*	**S**	**S**	**3**

Preglednica 7: *Komunikacijska oprema.*

GROŽNJA	STOPNJA GROŽNJE POGOSTOST (P)	STOPNJA RANLJIVOST STROŠKI (C)	TVEGANJE (vrednost iz tabele 3)
Naravna katastrofa *(potres, poplava, požar ...)*	**ZN**	**S**	**5**
Odpoved delovanja *(izpad elektrike, izpad delovanja lokalnega omrežja, onemogočen dostop)*	**N**	**N**	**6**
Oteženo delovanje *(nedostopnost do vseh podatkov, prekinjene povezave med podatki, virusi)*	**S**	**S**	**3**

GROŽNJA	STOPNJA GROŽNJE POGOSTOST (P)	STOPNJA RANLJIVOST STROŠKI (C)	TVEGANJE (vrednost iz tabele 3)
Namerna človekova dejavnost *(diverzija, sabotaža, stavka, kraja,namerno spreminjanje podatkov)*	**ZN**	**V**	**4**
Nenamerna človekova dejavnost *(napaka, površnost – neizkušenost posameznika, napačna navodila)*	**V**	**S**	**2**

Preglednica 8: *Podatki.*

6 UKREPI ZA ZMANJŠANJE STOPNJE TVEGANJA

Iz predstavljenih rezultatov analize stopnje tveganj po posameznih dobrinah je razvidno, da je glede na posamezne tipe groženj nivo tveganja zelo različen.

Ocenjujem, da so nekatera tveganja sprejemljiva in ne zahtevajo posebnih aktivnosti oz. intervencij. To so vsa tveganja, ki so v razpredelnicah označena s 5 in 6 – **majhno** tveganje.

Nekatera tveganja so ocenjena kot **povprečna** – označena s 3 in 4. To so že tveganja, ki zahtevajo določene ukrepe v smislu zmanjševanja tveganja – tako na področju pogostosti pojava kot tudi na področju stroškov. Odvisno od vrste dobrine bo za tovrstna tvegana treba izvesti ukrepe – priporočila, navodila, nadziranje delovanja in opozarjanje na nepravilno izvajanje.

Eno tveganje (na področju podatkov) je ocenjeno s kvalitativno oceno **veliko** – oznaka 2. Za tovrstno tveganje so potrebni takojšnji ukrepi – navodila, izobraževanje, spremljanje izvajanja.

Nobeno od tveganj ni ocenjeno z oceno **izredno veliko** – oznaka 1. Glede na naravo dela in glede na analizirane dobrine, bi taka ocena lahko pomenila pravo katastrofo tako s finančnega vidika kot tudi z vidika zaupanja v delovanje sistema geodetske uprave. Do tovrstnega tveganja na srečo ne prihaja iz dveh razlogov – zaradi zelo redke pogostosti posameznih groženj in ker so v sistemu že prisotni ukrepi, ki zmanjšujejo možnost napak oz. omejujejo posledice.

Predlagani ukrepi, ki so predstavljeni v nadaljevanju, so posledica opravljene analize in so tako sistemske kot tudi čisto operativne narave.

6.1 Osnovni varnostni dokument

Priporočila za pripravo informacijske varnostne politike je CVI, kot nosilna institucija na področju informatike v državni upravi, pripravil že v letu 2002. Prav tako je v letu 2002 Ministrstvo za okolje in prostor, predvsem na osnovi pobud in sodelovanja geodetske uprave, že pripravilo in izdalo pravilnik o postopkih in ukrepih za zavarovanje osebnih podatkov ter varovanju dokumentarnega gradiva (MOP, 2002). Kljub temu pa je na mestu ugotovitev, da geodetska uprava v splošnem še nima dokumenta, ki bi celovito urejal področje varovanja opreme in podatkov (postopki in ukrepi).

6.2 Zasnova centralnih baz podatkov – ločeni produkcijska in distribucijska baza

Za boljšo zaščito podatkov in predvsem bolj kakovosten in nemoten (neprekinjen) dostop do podatkov bo treba spremeniti osnovno zasnovo baz podatkov iz lokalnih v centralne baze. V okviru Projekta posodobitve evidentiranja nepremičnin se že izvaja poseben Projekt prenove centralne baze nepremičnin geodetske uprave, katerega osnovni namen je postavitev vsebinskega, procesnega in tehnološko enotnega informacijskega sistema, ki bo podpiral poslovanje z nepremičninskimi evidencami geodetske uprave in omogočal povezavo z ostalimi nepremičninskimi evidencami in drugimi evidencami (Mladenovič, 2002). Predvideno je, da bodo v okviru projekta na novo definirane osnovne baze podatkov na nivoju centralnih baz podatkov, predvsem pa bosta ločeni produkcijska in distribucijska baza podatkov.

6.3 Izobraževanje

Tako za celotno geodetsko upravo kot za vsako organizacijsko enoto velja, da bo treba povečati izobraževanje in seznanjanje vseh zaposlenih z ukrepi varovanja vseh dobrin informacijskega sistema geodetske uprave. To postaja še toliko bolj pomembno z uvajanjem novih e-storitev v poslovanju geodetske uprave kot tudi celotne državne uprave.

6.4 Operativni varnostni oz. zaščitni ukrepi

Poleg splošnih in za vse veljavnih ukrepov so kot rezultat analize za konkretno lokacijo OGU Kranj zanimive naslednje rešitve:

- zamenjava sedanjega UPS-napajalnika z močnejšim oz. priključitev na UPS-omrežje, ki ga je vzpostavila Mestna občina Kranj (v stavbi, kjer ima poslovne prostore tudi OGU Kranj),
- vgradnja avtomatskega detektorja požara oz. dima v vse poslovne prostore, najmanj pa v prostor, kjer je lociran strežnik,
- montaža sistema avtomatskega gašenja požarov v prostor, kjer je lociran strežnik,
- izboljšan sistem varovanega dostopa v poslovne prostore (vstop v poslovne prostore je sicer omejen s posebno magnetno kartico, vendar je uporaba nedosledna, v vse poslovne prostore lahko pride katera koli stranka – treba je torej zagotoviti poseben prostor, kjer bodo lahko stranke prišle v stik z upravo, oz. omejiti dostop do vseh prostorov),
- sprotno in dosledno izvajanje protivirusne zaščite in zagotavljanje sprotnega posodabljanja verzij tovrstnih programov,
- glede na širitev baz podatkov oz. vzpostavitev novih baz podatkov (npr. kataster stavb) je treba ponovno pregledati in rangirati nivo dostopov (uporabniška imena in gesla). Na tem področju bi bilo smiselno počasi uvesti službena spletna potrdila za nadzor do dostopa in uporabe informacijskega sistema geodetske uprave. To je sicer naloga, ki bi jo bilo treba izvesti na nivoju celotne geodetske uprave in ne samo za OGU Kranj.

7 ZAKLJUČEK

Ne samo geodetska uprava, tudi ostali državni organi nimajo izdelane celovite politike varovanja na področju informacijske tehnologije. To sicer ni opravičilo, je lahko vzpodbuda, da smo (še) na kakšnem področju lahko pred drugimi. Še posebej zato, ker za to področje že obstajajo določena priporočila (priporočila CVI). Samo enkratna izdelava »papirne« dokumentacije ni dovolj. Zagotavljanje varnosti na področju elektronskega poslovanja ni enkratno opravilo. Pomeni proces – stalno spremljanje predvidenih aktivnosti, izobraževanje in uvajanje novosti, ki jih omogočajo nove tehnologije in nova spoznanja. Vložek v zaščito sistemov sicer strmo narašča s stopnjo zahtevnosti zaščite (pri tem seveda ni dovolj gledati le na trenutni vložek, temveč na vložek v celem življenjskem ciklu). Največji in najtežje obvladljiv rizik predstavljajo zaposleni. Več zaščite prinaša tudi več komplikacij za uporabnike, ki pogosto v praksi potem povzročajo nove varnostne luknje, če politika ni celovita in podprta na vseh nivojih organizacije.

Analiza tveganja, ki je bila predstavljena v tem prispevku, je tako lahko le del celovite analize, ki bi jo bilo treba izvesti pred oz. v okviru izdelave celovite varnostne politike. Pri tem bi bilo treba pridobiti vse razpoložljive podatke in upoštevati vse možne dejavnike, ki lahko vplivajo na varnost sistema. To je in bo postalo še posebej pomembno, ker se e-poslovanje širi izredno hitro, se vpeljuje v vsakodnevno poslovanje javne uprave in postaja tudi eno od bistvenih komponent za uspešno poslovanje.

Literatura in viri

Evropska komisija (1999). Green Paper on Public Sector Information in the Information Society, URL: http:// 158.169.50.95:10080/info2000/en/publicsector/gp-index.html, Bruselj 1999.

Hajtnik, T. (2002). Priporočila za pripravo informacijske varnostne politike (za organe državne uprave), Center Vlade za informatiko, junij 2002.

Hudoklin, A., Šmitek, B. (1991). Varnost računalniško podprtega informacijskega sistema, Organizacija in kadri, 24, št. 9/10, str. 604–609.

Mladenovič, U. (2002). »Informacijski sistem nepremičninskih evidenc«, prezentacija, SIOUG.

Pravilnik o postopkih in ukrepih za zavarovanje osebnih podatkov ter varovanju dokumentarnega gradiva (2002). MOP, 20. 5. 2002.

Šmitek, B. (1992). Zagotavljanje varnosti računalniško podprtega informacijskega sistema, magistrsko delo, Univerza v Mariboru, Fakulteta za organizacijske vede.

Franc Ravnihar, univ. dipl. inž. geod.
Območna geodetska uprava Kranj, Slovenski trg 1, SI-4000 Kranj
E-pošta: franc.ravnihar@gov.si

Prispelo v objavo: 1. februar 2005
Sprejeto 19. februar 2005