UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

ANALIZA INFORMACIJSKE VARNOSTNE POLITIKE V AGENCIJI REPUBLIKE SLOVENIJE ZA KMETIJSKE TRGE IN RAZVOJ PODEŽELJA

Ljubljana, maj 2007 DAMJAN PETROVIĆ

IZJAVA

Študent/ka Damjan Petrović izjavljam, da sem avtor/ica tega diplomskega dela, ki sem ga napisala pod mentorstvom dr. Jurija Jakliča, in dovolim objavo diplomskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne 23.5.2007 Podpis:

KAZALO

1. UVOD

Informacije so postale del našega vsakdanjika na vseh področjih, tako v zasebni sferi kot tudi v poslovnem svetu. Ker predstavljajo zelo pomemben dejavnik delovanja podjetja in tudi samega obstoja, je potrebno dodeliti posebno pozornost njihovemu varovanju. Dejavniki, ki vplivajo na potrebo po varovanju informacij, so globalizacija, večja uporaba interneta, odpiranje podjetij navzven (čedalje več partnerjev in vsakodnevnega posodabljanja poslovanja) (Micro Process d.o.o., 2007).

Na področju razvoja telekomunikacijske, komunikacijske in računalniške tehnologije se odpirajo čedalje večje možnosti za učinkovitejšo in cenejšo uporabo ter obdelavo raznovrstnih informacij na eni strani ter na drugi strani čedalje večje možnosti za zlorabo, uničenje in poneverbo podatkov. Same motnje v delovanju komunikacijske in računalniške opreme pa lahko povzročijo izpad poslovanja podjetja in s tem neprecenljivo škodo. Vsa ta dejstva pa so privedla do tega, da morajo uporabniki povečati informacijsko in računalniško varnost.

Če pa gre ustanovo ki upravlja z ogromno količino osebnih podatkov, kot je Agencija Republike Slovenije za kmetijske trge in razvoj podeželja, pa mora biti ta varnost podatkov še na toliko višjem nivoju. Vsakodnevno se mora agencija boriti proti raznim varnostnim incidentom, ki prihajajo tako od znotraj kot tudi od zunaj. Ta najvišji nivo pa zaenkrat predstavlja standard BS 7799. Vendar pa to ne pomeni, da se kupi na trgu tak sistem, ki je v skladu s standardom BS 7799 in da bo ta sistem deloval tako, kot mora. V sam razvoj je potrebno stopiti organizirano in sistematično.

Namen diplomske naloge je prikaz organiziranosti varnostne politike v Agenciji Republike Slovenije za kmetijske trge in razvoj podeželja. Poudarek je na analizi te varnostne politike in na prikazu, kaj bi lahko bilo bolje skozi oči uporabnika tega sistema.

Najprej sem predstavil kaj sploh je varovanje informacij, pomembnost le-tega in glavne tipe groženj, ki ogrožajo vsako podjetje. V naslednjem poglavju sem predstavil sam varnostni standard BS 7799 in podal glavne značilnosti le-tega. V četrtem poglavju pa sem opisal koncept varnostne politike, kakšno je načrtovanje te politike in vpeljevanje v uporabo. Osredotočil sem se za večnivojsko urejeno varnostno politiko, ker je ta tudi značilna za ARSKTRP. Vsa ta poglavja so predstavljala nekakšno podlago praktičnemu delu in tudi sami analizi varnostne politike. Praktični del diplome sem začel s splošnim opisom Agencije Republike Slovenije za kmetijske trge in razvoj podeželja. Prikazal sem, kako je urejena varnostna politika v tej agenciji. Nato sem analiziral samo varnostno politiko ARSKTRP po področnih varnostnih politikah, ki zopet izhajajo iz BS 7799, kjer sem prikazal bolj podrobno področje administracije uporabnikov, katero sem tudi sam opravljal. Po pogovorih z zaposlenimi, ki so doživeli spremembe uvajanja nove varnostne politike, sem prikazal do kakšnih težav je na splošno prihajalo. Na koncu sem seveda podal svoje mnenje o tem, kako bi se lahko določene stvari izboljšale.

2. VAROVANJE INFORMACIJ

2.1. Kaj je varovanje informacij

Informacije so poleg kapitala, ljudi, naravnih virov in znanja zelo pomemben vir za poslovanje podjetja in še vedno pridobivajo na vedno večji pomembnosti. Zato je potrebna vzpostavitev ustreznih sistemov varovanja informacij na temelju varnostnih standardov, zakonodaje in razpoložljive informacijske tehnologije. Osnovna naloga varovanja informacij je zaščita le-teh pred različnimi nevarnostmi iz okolja, kot tudi iz podjetja samega in zagotavljanje neprekinjenega poslovanja ter omejitev poslovne škode na najmanjšo možno raven. Samo varovanje informacij bo učinkovito le takrat, ko se bo sistem varovanja uporabljal na primeren in pravilen način, da bo prinašalo koristi (zmanjšuje stroške in povečuje produktivnost) (Horjak, 2005).

Varovanje informacij zajema predvsem zagotavljanje naslednjih treh osnovnih načel (BS/IEC 17799:2000):

- **Neoporečnost:** varovanje točnosti in popolnosti informacij ter računalniške programske opreme. Podatki, s katerimi se upravlja, morajo biti vredni zaupanja.
- **Zaupnost:** zagotavljanje, da so informacije dostopne samo pooblaščenim osebam. Nanaša se na vse podatke, ki so direktno povezani s programskimi rešitvami, z nosilci podatkov, komunikacijske in ostale procese.
- **Razpoložljivost:** zagotavljanje, da so informacije in računalniške storitve na voljo pooblaščenim uporabnikom, kadar jih potrebujejo. Poslovni partnerji pričakujejo hiter in zanesljiv dostop do potrebnih podatkov. Je vitalnega pomena za organizacijo.

Informacije, ki so potrebne varovanja, se ugotovijo s popisom sredstev. Temu pa sledi analiza tveganj. Na podlagi te analize se pripravijo ukrepi za zmanjševanje tveganj in nadzor njihove uporabe. Vsi ukrepi (načini dela, postopki, organizacijska struktura in funkcije programske opreme) se zapišejo v dokument varnostne politike, ki za vsako posamezno področje ali problem natančno določa, kako ukrepati. Z vsebino varnostne politike morajo biti seznanjeni vsi zaposleni. Zelo pomembno je, da varovanje informacij izhaja iz ciljev organizacije.

2.2. Pomembnost varovanja informacij

Neoporečnost, zaupnost in razpoložljivost informacij lahko igra bistveno vlogo pri ohranjanju konkurenčnosti, denarnih tokov, dobičkonosnost, usklajenosti z zakonom ter pri ohranjanju komercialne podobe (BS/IEC 17799:2000). Informacije so vse lažje dosegljive vedno večjemu številu ljudi, zato se vzporedno povečujejo tudi možnosti zlorab (računalniške prevare, vohunstvo, sabotaže, zlonamerna koda...), povečuje pa se tudi količina podatkov in to v tej meri, da se ta količina podvoji vsako drugo leto.

Na drugi strani pa lahko grozijo delovanju ali celo obstoju podjetja razne odpovedi sistemov in napake v programih. V zadnjem času so najpogostejši vzroki za uvedbo sistema varovanja informacij razne zahteve revizij, vladnih agencij in centralne banke. Dobro in kvalitetno organiziran sistem varovanja informacij lahko vsa ta tveganja zmanjša na sprejemljivo raven. Samo varovanje pa pomembno vpliva tudi na delovne procese. Onemogoča razne prekinitve v poslovanju, ki so lahko povzročene namerno ali nenamerno, se pravi, da omogoča neprekinjen proces poslovanja.

2.3. Dejavniki, ki ogrožajo informacijske sisteme

Nevarnost preži na vseh področjih delovanja podjetja, kot tudi v delovanju posameznika. Na eni strani gre za nevarnost, povezano z naključnimi dogodki, kot so razne napake uporabnikov, napake v strojni opremi ali napake v samem informacijskem sistemu in razne naravne nesreče ter požare. Na drugi strani pa preži nevarnost, ki je povezana z namerno povzročeno škodo. Sem spadajo zlonamerna koda, socialni inženiring, razni vsiljivci, ponaredbe in kraje.

2.3.1. Namerno povzročena škoda

V današnjem svetu, v katerem je pomembna le konkurenčna prednost, prihaja velikokrat do namernega vdiranja v sisteme. Do tega prihaja iz različnih vzrokov. Na eni strani se to počne zaradi pridobivanja podatkov, ki bi lahko zelo pomagali v konkurenčnem boju, na drugi strani pa imamo tako imenovane »hekerje«, ki vdirajo v sisteme zaradi dolgočasenja ali preprosto zaradi dokazovanja svojega znanja. Posledice se lahko kažejo v uničenju virov, poškodovanju informacijskega sistema in izgubi zaupnosti, neokrnjenosti, razpoložljivosti, pooblaščenosti ali zanesljivosti (BS ISO/IEC TR 13335-1, 1996, str. 8). Obstajajo razni načini, kako škodovati podjetjem, kot so zlonamerna koda, socialni inženiring, razne kraje in ponaredbe...

2.3.1.1. Zlonamerna koda

Pod pojmom *zlonamerna koda* razumemo:

- viruse,
- črve,
- trojanske konje,
- vohune in drugo nezaželeno kodo.

Glavni namen piscev take kode je povzročanje škode, izgube podatkov, vohunjenje ali preprosto zgolj dokazovanje svojega znanja. Take kode povzročajo veliko škodo zaradi izpadov sistemov, kot tudi zaradi časa, ki ga zaposleni porabijo za njihovo odstranitev in vzpostavitev ponovnega delovanja prizadetih sistemov. Nujno je, da ima organizacija vgrajene naprave in postopke, ki omogočajo zaščito podatkov (Damij, 1995).

Virus je bolj ali manj preprost računalniški program, ki posnema nekatere značilnosti bioloških virusov in se prilepi v gostiteljski program in ki lahko povzroči škodo v

strojni in programski opremi ter v datotekah. Najpogostejša oblika širjenja virusov je s priponkami v elektronski pošti ali preko brezplačnih vsebin na internetu, ki jih prenesemo na svoj računalnik v obliki dokumentov, programov, slike, glasbe (Frangež, 2006). Poznamo več vrst virusov. Nekateri kažejo samo drugačno zaslonsko sliko, nekateri igrajo glasbo. Na drugi strani pa imamo tudi viruse, ki upočasnijo delovanje sistema ali še hujše, ki pa spreminjajo podatke ali jih celo brišejo. Virusi se zelo hitro širijo. V današnjem času se lahko v manj kot 24 urah razširijo že po celem svetu.

Črvi so programi s sposobnostjo kopiranja samega sebe iz enega računalnika v drugega. Navadno to počnejo preko računalniških omrežij (Frangež, 2006). Črvi ne okužijo datotek, pač pa ostanejo aktivni v delovnem pomnilniku, od koder se skušajo preko pošte ali omrežja razširiti na čim več računalnikov. Ti programi izkoriščajo napake v operacijskih sistemih in se na tak način namestijo v računalnik. Črvi lahko spreminjajo oziroma brišejo podatke, lahko pa napadejo druge računalnike preko našega. Najpogostejša oblika širjenja črvov je preko elektronske pošte, kjer si črv pomaga z uporabnikovo zbirko naslovnikov. Lahko pa se širijo tudi preko map v skupni rabi.

Pri **trojanskem konju** gre za samostojen izvršljiv program, ki vsebuje uničujočo kodo in svojemu lastniku omogoča popoln dostop do napadenega računalnika ali vsaj omogoči prenos pomembnih osebnih podatkov. Največkrat se v elektronski pošti pritihotapi v računalnik ali preko raznih klepetalnic. Najbolj znana sta Back Office in NetBus. Zelo težko jih je odkriti, ker gre za zelo majhne in v kodi drugega programa skrite tvorbe. Najboljša obramba proti trojanskim konjem je redno osveževanje in posodabljanje antivirusnih programov ter redno nalaganje zadnjih popravkov operacijskega sistema.

Glavna vloga **vohuna** je prisluškovanje prometu, ki se pretaka po omrežju. Nelegalno se uporabljajo za pridobivanje tajnih podatkov in gesel. Legalno pa jih uporabljajo sistemski upravitelji za prikaz stanja omrežja, iskanje morebitnih napak in porazdelitev obremenjenosti omrežja. Najboljša obramba je kodiran promet, kajti vohunov se skoraj ne da izslediti. Ena taka oblika vohunov so opazovalci tipkovnic (ang. Keylogger), ki si zapomnijo tipke, ki jih tipkamo, in na ta način lahko pridejo do raznih uporabniških imen in gesel. V obdobju med januarjem in novembrom 2005 so pri podjetju Sophos odkrili 16.000 novih virusov, črvov in trojanskih konjev, kar je 48 odstotkov več kot v letu 2004 (Frangež, 2006). Največ groženj je bilo v obliki trojancev z 62 odstotkov, črvi pa so bili zastopani s 35 odstotki.

2.3.1.2. Socialni inženiring (manipulacija)

Gre za najcenejši in tudi najenostavnejši napad na informacijske sisteme. Izkorišča človeško nevednost, pomanjkanje izkušenj ali lahkomiselnost. V velikem številu primerov se je napadalec izdajal za serviserja in je na tak način pridobival razna vstopna gesla in s tem pomembne podatke. Čeprav zahteva taka manipulacija majhne denarne vložke, lahko povzroči ogromno škodo. Problem se pojavi tudi zato,

ker v tem primeru ne delujejo klasična orodja varovanja.Glavni protinapad socialnemu inženiringu je vlaganje v stalno izobraževanje in osveščanje zaposlenih.

2.3.1.3. Kraja in nezakonito razmnoževanje intelektualne lastnine

Nezakonito razmnoževanje in prodaja intelektualne lastnine z namenom pridobitve večje protipravne premoženjske koristi se obravnava kot kriminalno dejanje in se preganja po 159. členu kazenskega zakonika Republike Slovenije.Podjetja morajo varovati svoje informacije, saj lahko njihove skrivnosti in lastni recepti do uspeha hitro preidejo v roke konkurentov.

2.3.1.4. Vsiljivci (ang. Intruders)

To so vsi nepooblaščeni vstopi v informacijski sistem. Uporabniki se v sistem pretihotapijo s pomočjo zlonamernih kod ali vohunov in na ta način pridobivajo podatke ali pa samo izkoristijo vire informacijsko-komunikacijskega sistema. Proti njim se je možno boriti s pomočjo orodij za preprečevanje vdora v sistem.

2.3.1.5. Ponaredbe in kraje

V tem primeru gre v za kaznivo dejanje. Večina takih poneverb je izvedena s strani zaposlenih, saj imajo dostop do računalniških sistemov in jih tudi dobro poznajo. Tiste poneverbe in kraje, ki se zgodijo s strani zunanjih uporabnikov, pa zahtevajo več izkušenj in znanja, ki ga ponavadi posedujejo tako imenovani »hekerji«. Nekateri vdori se zgodijo zaradi pridobitniških namenov, nekateri pa zaradi dokazovanja posameznikov v smislu, da lahko naredijo karkoli, če se jim to zahoče. Sistem varovanja bo učinkovit takrat, ko bo škodljivcem povzročal več stroškov kot pa koristi s krajo ali ponaredbo.

2.3.2. Napake

Napake se pojavljajo na različnih področjih. Lahko se pojavijo na strojni opremi, lahko se pojavijo v programski opremi. Na drugi strani pa se pojavljajo tudi napake na strani uporabnikov ali pa napake v podatkih.

2.3.2.1.Napake strojne opreme

Take vrste napak se kljub visoki zanesljivosti še vedno lahko dogajajo in to največkrat zaradi pregrevanja, tresljajev, vlage… Največkrat se zaradi odpovedi enega od podsistemov zaradi varnosti ustavi celoten sistem. Izjema je oprema, kjer so vitalni deli podvojeni. Sistem, ki je v primeru izpada nadomestni sistem, je lahko v fazi delovanja primarnega sistema pasiven, lahko si delita naloge ali pa opravlja popolnoma druge naloge.

2.3.2.2.Napake v programski opremi

Pogosto se pojavijo šele ob sami uporabi programske opreme. Te napake so posledica obsežnosti in vse krajših rokov izdaje programske opreme, ki se v celoti ponavadi ne testira. Običajno sta produkcijsko in testno okolje ločena.

2.3.2.3. Napake uporabnikov

So najpogostejši vzrok nepravilnosti v delovanju informacijskih sistemov. Navadno gre za površnost pri delu, neupoštevanje navodil organizacij. Zaradi same narave teh napak se ne da nikoli predvideti vseh možnosti za preprečitev. Običajno so površni uporabniki tudi vzrok za **napake v podatkih.** Ne glede na kvaliteto posameznega informacijskega sistema bo ta vedno občutljiv na napake uporabnikov.

2.3.3. Nesreče

Velik problem pri nesrečah je ta, da jih ne moremo predvideti. Naravne nesreče, kot so udari strel, potresi, poplave, so poleg tega, da jih ne moremo predvideti, še take, da na njih nimamo nobenega vpliva. Vendar moramo kljub tem dejstvom narediti vse, da te dogodke predvidimo in tako tudi oblikujemo sistem varovanja podatkov. Na požare smo ponavadi zelo dobro pripravljeni, ker tako zahtevajo gradbeni predpisi in se tudi pojavljajo pogosto. Na drugi strani pa premalo ljudi da poudarek na obrambo pred možnostjo izliva vode. Razni vodovodni problemi v stavbi lahko zelo hitro poplavijo sistemsko sobo in s tem uničijo pomembne podatke. Ta problem se lahko reši na preprost način: oprema v sistemski sobi se dvigne od tal in tako zmanjša možnost poškodbe zaradi vdora vode v prostor.

2.4. Zahteve po varovanju informacij

Vsaka organizacija mora imeti za zaščito pomembnejših poslovnih procesov vpeljan proces, ki omogoča poslovanje, ki ne bo prekinjeno ob vsakem izpadu informacijskega sistema. Ta jo ščiti pred učinki večjih napak ali katastrof, s tem pa zmanjšuje prekinitev dela na sprejemljivo raven (BS ISO/IEC 17799:2000, 2000).

Upravljanje neprekinjenega poslovanja mora biti sestavni del upravljanja podjetja. Načrtovanje in vzpostavljanje neprekinjenega poslovanja je tesno povezano z vsemi poslovnimi procesi v organizaciji. V praksi velikokrat srečamo dejstvo, da je načrtovanje teh aktivnosti prepuščeno samo tehničnemu osebju s področja informatike in zato največkrat ne nudi celovitega odgovora organizacije na tveganja, katerim je izpostavljena. To dejstvo nam znova dokaže, da se je treba lotiti varovanja podatkov celovito. Organizacija mora objaviti sprejeto politiko in smernice za upravljanje neprekinjenega poslovanja in seveda poskrbeti za njeno pravilno izvajanje.

Podjetja, vladne ustanove in bančne institucije se največkrat odločajo za varovanje informacij zaradi poslovnih in tudi zakonskih zahtev. Informacijska varnost je v močni

povezavi z informacijskim pravom. Tu se začnejo odpirati vprašanja s področja dostopa do programske, strojne in sistemske opreme, varstva osebnih podatkov, kriptiranja, elektronskega poslovanja in podpisovanja, intelektualne lastnine... (Berčič, 2003).
Zakoni, ki v Sloveniji opredeljujejo varovanje informacij, so (Makarovič et al., 2001):

- Zakon o elektronskem poslovanju in elektronskem podpisu;
- Zakon o elektronskih komunikacijah;
- Zakon o varstvu osebnih podatkov;
- Zakon o avtorskih in sorodnih pravicah;
- Zakon o pogojnem dostopu do zaščitenih elektronskih storitev;
- Zakon o varstvu potrošnikov,
- Zakon o tajnih podatkih.

Tudi sam trg zahteva od podjetij, da uredijo svojo varnostno politiko. Podjetja, ki imajo dobro organizirano varnost, so še vedno ogrožena preko poslovanja s podjetji, ki tega nimajo najbolje urejenega.

Zavarovalnice v tujini se že ukvarjajo z zavarovanjem pred nevarnostmi elektronskega poslovanja. Vendar pa je potrebno vedeti, da zavarovanja za vrednost podatkov na notranjih pomnilnikih ne bo sklenila nobena zavarovalnica, če ne bo prej dokazano, da je poskrbljeno za dnevno osvežene kopije podatkov in pravilno delovanje informacijskega sistema.

3. STANDARD BS 7799

3.1. Splošne značilnosti standarda BS 7799

Je mednarodno priznan standard, namenjen obvladovanju varnosti na organizacijskem nivoju. Predstavlja model za učinkovit sistem upravljanja varovanja informacij (SUVI) in je uporaben v vseh industrijskih panogah. Prenosljiv je v različna okolja in primeren za različne velikosti organizacij (Zupan, 2006, str.14). Sestavljen je iz dveh delov. Prvi del kaže najboljšo prakso pri zadovoljevanju zahtev standarda in podaja razlago, kaj naj bi organizacija imela. V drugem delu najdemo specifikacijo z napotki za uporabo. Tu je tudi razlaga, kaj mora organizacija narediti, da bo skladna s standardom. Standard podpira procesni pristop k zasnovi, vpeljavi, izvedbi, nadziranju, vzdrževanju in izboljševanju učinkovitosti SUVI v organizaciji.

Standard je sestavljeni iz 10 poglavij, 36 ciljev, 127 kontrol.

Glavna poglavja standarda so (BS 7799-2:2002):

1. Varnostna politika (BS7799-2 A.3)
2. Organizacijska varnost (BS 7799-2 A.4)
3. Klasifikacija sredstev in kontrola (BS 7799:2.DEL – A.5)
4. Varnost osebja (BS 7799: 2. DEL – A5)
5. Fizična zaščita in zaščita okolja (BS 7799: 2. DEL – A.7)

6. Upravljanje s komunikacijami in s produkcijo (BS 7799: 2. DEL – A.8)
7. Nadzor dostopa (BS 7799-2 – A.9)
8. Razvijanje in vzdrževanje sistemov (BS 7799-2 – A.10)
9. Upravljanje neprekinjenega poslovanja (BS 7799-2 – A11)
10. Združljivost (BS 7799-2 – A.12)

Cilj prvega poglavja je zagotovitev, da vodstvo organizacije usmerja in podpira varovanje informacij. Vodstvo organizacije naj bi z objavo in zagovarjanjem politike varovanja informacij določila jasno in taktično usmeritev. Celotni organizaciji mora biti pokazano, kako pomembna je predanost varovanju informacij po celi organizaciji.

Drugo poglavje govori o organiziranosti varovanja. Poudari potrebo po oblikovanju varnostnega foruma, katerega namen je skrb za smernice varnostne politike v organizaciji.

V tretjem poglavju je glavna točka popis vseh sredstev, ker se edino tako lahko določi lastništvo nad pomembnejšimi sredstvi in določi odgovornost za vzdrževanje ustreznih kontrol.

V četrtem poglavju izvemo, kako zmanjšati tveganje zaradi človeških napak, kraj, poneverb ali zlorab zmogljivosti. To pa rešijo razna usposabljanja zaposlenih, izobraževanje in redno dopolnjevanje znanja o varnostnih politikah, preverjanje oseb preden se zaposlijo in preverjanje pogodbenih strank...

Peto poglavje je namenjeno fizičnemu varovanju, predvsem varovanju vitalnih informacijskih sredstev: zaščita sredstev pred nepooblaščeno uporabo, ločenost območja za dostavo od zmogljivosti za obdelavo informacij, zaščita opreme pred naravnimi in drugimi nesrečami...

V šestem poglavju je obravnavana varnost omrežij in računalnikov. Najdemo lahko tudi navodila za pravilno uporabo le-teh, postopke za zaščito pred zlorabo informacij. Ločiti se morajo testne in produkcijske zmogljivosti, potrebno je redno preverjanje varnostnih kopij pomembnih poslovnih informacij in programske opreme. Opredeljeni so tudi načini in postopki o uničenju nosilcev podatkov, ki jih več ne potrebujemo…

Sedmo poglavje govori o tem, kako se mora ravnati z dostopi do sistema, o dodeljevanju pravic, gesel, o varnosti podatkov in računalniške opreme, ko ti niso v uporabi, o dostopu zaposlenih samo do tistih stvari, ki jih nujno potrebujejo za delovanje…
Osmo poglavje je namenjeno razvoju in vzdrževanju informacijskega sistema še posebej z vidika varnosti aplikacij, datotek preko kriptiranja. Prikaže nam tudi kako mora biti urejeno varovanje sistemskih datotek in kakšen naj bo nadzor nad programi v izvorni kodi.

Deveto poglavje se nanaša na pomembnost zagotavljanja neprekinjenega poslovanja in na zaščito kritičnih poslovnih procesov pred večjimi okvarami in nesrečami.

Deseto poglavje pa obravnava usklajenost informacijskega sistema z zakonodajo, tako na področju pravnih zahtev, kot tudi varnostnih pregledov informacijskega sistema (Konečnik, 2002).

Standard in sistem za upravljanje varovanja informacij je postal stalna praksa v številnih mednarodnih podjetij in se uveljavlja v vedno večjem številu. ISO/IEC 17799:20 je pripomoček za ugotavljanje varnostne skladnosti, medtem ko je BS7799-2:2002 podlaga za certificiranje. Podjetje, ki se želi certificirati po BS7799 standardu, mora dokazati, da so izbrane varnostne kontrole ustrezne in primerno ščitijo pred prepoznavnimi tveganji. V Sloveniji je uvajanje standarda in certificiranja v porastu.

V letu 2005 je standard ISO/IEC 27001 nadomestil standard BS 7799-2:2002. Gre za manjše razlike. Razlike najdemo v 17 novih ter številnih spremenjenih, dopolnjenih, združenih ali odstranjenih kontrolah (Knez, 2005, str. 18).

Vedno več podjetij se zaveda pomena uvajanja varovanja informacij s pomočjo standarda BS 7799. Nekatera izmed večjih podjetij v Sloveniji, ki so uvedla Sistem upravljanja varovanja informacij po standardu BS 7799, so Fructal, banka Sparkasse, podjetje Iskraemeco, Nova Ljubljanska banka d.d. (Varnostni forum, 2007).

3.2. Sistem za upravljanje varovanja informacij (SUVI)

Sistem za upravljanje varovanja informacij (v nadaljevanju SUVI), ali (ang. ISMS – Information security management system) je vodstveni sistem in je osnova standarda BS 7799. Njegov namen je skrb za vpeljavo, vzdrževanje in izboljševanje informacijske varnosti v organizaciji. Na tak način prepozna tveganja, s katerimi se vsakodnevno srečuje in jih zmanjša na želeno raven. S tem dokazuje, da zna pravilno ravnati z informacijami, da se zna pravilno odzivati v primeru informacijskih nesreč ter omiliti posledice, ki lahko vplivajo na poslovanje (Krkoč, 2006, str. 12). Zelo pomembno je, da je ta sistem usklajen s cilji, ki jih želi doseči organizacija na vseh področjih poslovanja. Bistvenega pomena je tudi to, da organizacija v SUVI vidi poslovne priložnosti, kot so (Berčič, 2003a):

- Zadovoljevanje potreb trga v skladu s kakovostjo in varnostjo, ki jo organizacija obljublja;
- obvladovanje lastnih poslovnih procesov in dejavnikov;
- stalno izboljševanje kakovosti in varnosti poslovanja;
- zmanjševanje poslovnih in operativnih tveganj.

SUVI je sestavljen iz štirih faz. Te faze so:

- **N**ačrtuj
- **S**tori
- **P**reveri
- **U**krepaj

Gre za procesni pristop načrtuj-stori-preveri-ukrepaj (NSPU) in je značilen za vse ostale upravljavske sisteme. V nadaljevanju bom predstavil posamezne faze sistema za upravljanje varovanja informacij.

3.2.1. Faze SUVI

Aktivnosti modela »načrtuj-stori-preveri-ukrepaj« so naslednje (BS 7799-2:2002, str. 7-8):

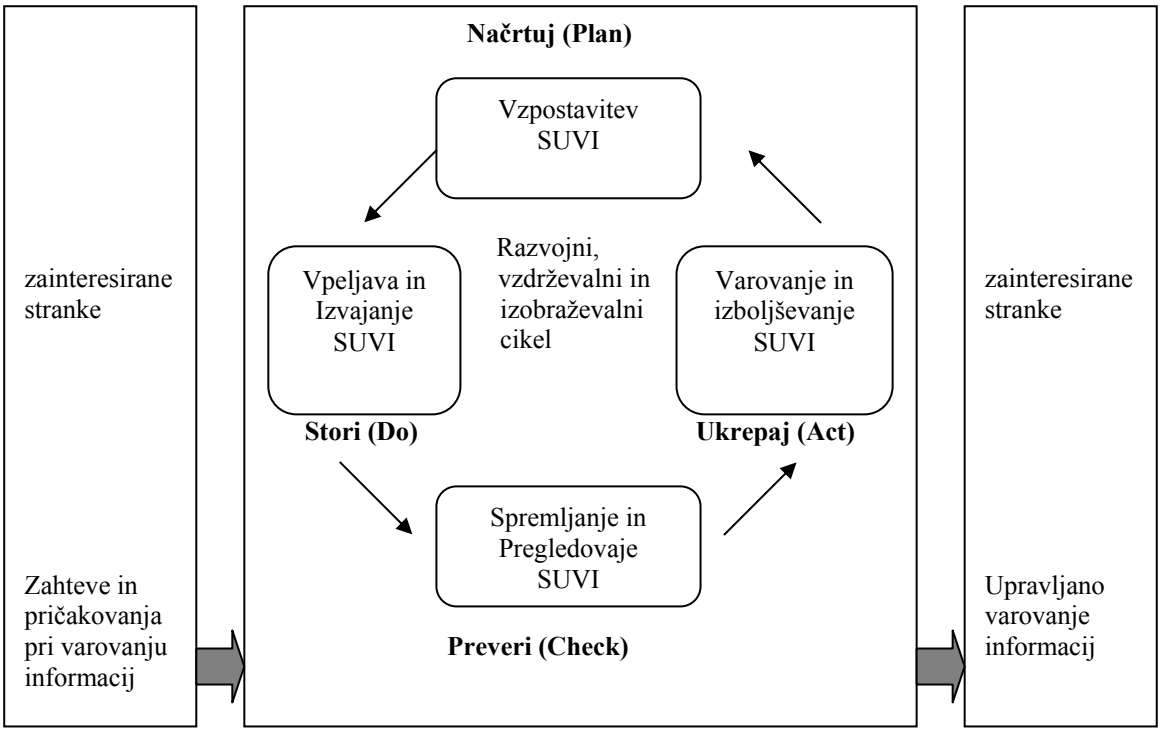
Načrtuj (zasnova SUVI)
Določitev varnostne politike, namenov, ciljev, procesov in postopkov, ki so pomembni za upravljanje s tveganji in ki dajejo rezultate v skladu s splošno politiko in cilji organizacije.

Stori (vpeljava in izvajanje SUVI)
Vpeljava in izvajanje varnostne politike, kontrol, procesov in postopkov.

Preveri (spremljanje ter pregled SUVI)
Ocenjevanje in, kjer je izvedljivo, tudi merjenje delovanja procesov glede na varnostno politiko, cilje in praktične izkušnje, ter poročanje o dobljenih rezultatih vodstvu organizacije, ki naj jih pregleda.

Ukrepaj (vzdrževanje ter merjenje, analize in izboljševanje SUVI)
Na osnovi rezultatov pregleda vodstva se sprejmejo popravni in preventivni ukrepi, ki pripomorejo k nenehnemu izboljševanju SUVI.

Slika 1: Model NSPU za proces SUVI



Vir: BS7799-2:2002, 2002, str. 8.

Na sliki vidimo, da SUVI kot vhodno sredstvo sprejme zahteve in pričakovanja po varovanju zainteresiranih strank ter s potrebnimi dejanji in postopki izdela izhodna sredstva za varovanje informacij, ki izpolnjujejo te zahteve in pričakovanja.

SUVI vsebuje tudi kodeks varovanja informacij. Z njim podaja organizacijam priporočljive smernice informacijskih kontrol, ki jih podjetja vpeljejo za zaščito svojih virov. S specifikacijami za sistem upravljanja in varovanja informacij pa standard ponuja navodila za uvajanje osnovnih varnostnih mehanizmov za prepoznavanje virov, potrebne stopnje varnosti in podobno. Standard predlaga 127 kontrol in 36 ciljev kot priporočila za začetek načrtovanja in vpeljevanja varnosti. Odločitvi posameznega podjetja pa je prepuščeno to, katere izmed kontrol bodo izbrane.

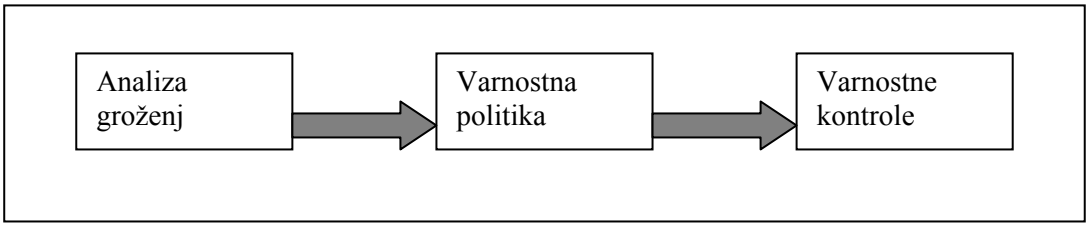
4. VARNOSTNA POLITIKA

Varnostna politika nudi odgovor na dejavnike, ki ogrožajo informacijski sistem od zunaj, kot tudi na dejavnike, ki ogrožajo sistem od znotraj. Ob upoštevanju smernic, ki jih navaja varnostni standard BS 7799, pa bomo lahko tudi prepričani v njeno učinkovitost, saj ima standard pokrite vse vidike poslovanja ene organizacije.

Varnostna politika je program varnosti in je v pristojnosti vodstva. V tem programu so definirani cilji, pravila in odgovornosti v zvezi z varnostjo informacijskih virov podjetja, razni postopki in pravila. Program obsega pravila o fizičnem in tehničnem varovanju ter pravila, s katerimi je določeno, kakšni bojo načini varovanja. Vsako dejanje, pa naj gre za namerno ali nenamerno, ki ne upošteva pravil, določenih v varnostni politiki, se obravnava kot kršenje varnostnih pravil. Dobra varnostna politika ima dovolj informacij o tem, kaj je potrebno postoriti za zaščito informacij, virov in ljudi v podjetju. Sestavljena je iz skupka varnostnih pravil, s katerimi morajo biti seznanjeni vsi zaposleni. Ta pravila opredeljujejo način obnašanja, odgovornosti, naloge in splošna pravila za delo zaposlenih.

Skrbniki informacijskih virov in poslovnih procesov morajo biti pri oblikovanju varnostne politike pozorni na grožnje, ki prežijo iz okolja in iz podjetja samega (Beganovič, 2004, str. 67). Prepoznava in vpeljava ustreznih zaščit zahteva sistematično planiranje in podporo vseh zaposlenih v podjetju. V fazi načrtovanja in opredeljevanja varnostne politike je potrebno gledati na velikost podjetja, razpoložljivost finančnih sredstev in stopnjo ogroženosti, ker naj bi potem izboljšala razpoložljivost, celovitost in zaupnost znotraj in zunaj podjetja. V tej fazi se uporabijo rezultati predhodno narejene ocene tveganj, kjer so se prepoznale vse potencialne grožnje. Popis teh groženj bo osnova za opredelitev varnostne politike. Po opredelitvi pa se začne izbira varnostnih kontrol. Sestavljena je iz skupka varnostnih pravil, s katerimi morajo biti seznanjeni vsi zaposleni. Ta pravila opredeljujejo način obnašanja, odgovornosti, naloge in splošna pravila za delo zaposlenih.

Slika 2: Vloga varnostne politike



Vir: Olovsson, 1992, str. 7.

Varnostna politika zajema širok krog varnostnih vprašanj, ki so za vsako podjetje drugačna. Zaradi tega in zaradi specifičnosti poslovanja vsakega podjetja pa pripravljenega dokumenta varnostne politike ni mogoče kar kupiti v trgovini. Iz tega sledi, da mora vsako podjetje razviti svojo varnostno politiko, v kateri bodo upoštevani vsi dejavniki poslovanja podjetja. Eden od takih pomembnih dejavnikov je značilnost lastnega informacijskega sistema. Prav ta dejavnik pa mora biti upoštevan, če hočemo razviti optimalno delujočo varnostno politiko. Pri razvoju morajo biti vključeni strokovnjaki z različnih področij delovanja podjetja.

Standard BS7799 omenja varnostno politiko le kot eno izmed priporočenih kontrol, ne spušča pa se v podrobna priporočila za pripravo politike (Beganović, 2004, str. 67). Politika mora biti v pisni obliki in kot taka na voljo vsem zaposlenim, ki so odgovorni za varovanje informacij. Vodstvo je odgovorno za potrditev dokumenta in za seznanjanje zaposlenih o varnostni politiki. Določi se lastnik dokumenta in ta je zadolžen za njegovo vzdrževanje in preglede.

4.1. Načrtovanje varnostne politike

Pogoj za razvoj celovite varnostne politike je poznavanje in popolno razumevanje poslovanja podjetja ter delovanja informacijskega sistema v tem podjetju. Nastajajoča varnostna politika mora upoštevati vse obstoječe politike in pravila, predpise in zakonske zahteve, ki so razviti v podjetju. V tej fazi se morajo najprej določiti vloge in odgovornosti ekipe, ki bo sodelovala v razvoju in vpeljavi varnostne politike. Določi se primarnega vodjo projekta, ki je ponavadi kar varnostni inženir podjetja, ki je odgovoren za uspešno izvedbo tega projekta. Določijo se tudi ostali udeleženci, ki bodo sodelovali pri tem projektu. To so: lastniki procesov, pravniki, kadrovska služba, tehnično osebje… Zelo pomembno je, da si zastavimo smernice načrtovanja varnostne politike in si odgovorimo na naslednja vprašanja (Kee, 2001, str. 2): »Katere podatke in informacijske vire želimo zaščititi?, Pred kom jih želimo zaščititi?, Na kakšen način jih bomo zaščitili?, Koliko smo za zaščito pripravljeni investirati?«.

Skozi proces ocenjevanja tveganja se opredelijo informacijski viri in poslovni procesi ter naredi popis interakcij med viri in poslovnimi procesi. Temu procesu sledi ovrednotenje virov, kjer se vsakemu viru določi stopnja vrednosti, prepoznavanje ranljivosti virov in groženj ter v končni fazi ocena tveganja. S pomočjo popisa groženj

se preverijo obstoječe varnostne kontrole ter potencialne varnostne kontrole in strošek njihove uvedbe. Popis rezultatov in priporočil za zmanjšanje tveganja predstavlja zelo dobro osnovo za dokumentiranje varnostne politike.

4.2. Vpeljevanje varnostne politike

Aktivna vloga uporabnikov pri razvoju varnostne politike je zelo pomembna, saj bo edino tako sprejeta med zaposlenimi in s tem se bo zmanjšalo izmikanje pravilom le-te. Zelo pomembno vlogo igra tudi samo izobraževanje zaposlenih o potrebi po varovanju virov in informacij, ki so pomembne za podjetje.

Razviti je potrebno ustrezne metode, s katerimi bo omogočeno preverjanje usklajenosti z varnostno politiko. Eden izmed načinov je določitev notranje skupine za nadzor, ki bo zagotavljala izvajanje varnostne politike ter preverjala razumevanje in zavedanje pomembnosti politike varovanja med zaposlenimi. Notranji nadzorniki, ki so odgovorni za spremljanje usklajenosti z varnostno politiko, morajo biti neodvisni od izvajalcev, ki so to politiko vpeljali.

Drugi način je vpeljava avtomatiziranih orodij, katerih namen je pregledovanje datotek za beleženje različnih dogodkov, na primer prijavljanja v sistem in omrežje, pravilne in pooblaščene uporabe informacijskih virov. Temu sledi kontinuirano pregledovanje in nadzor nad vsemi dogodki v informacijskem sistemu zaradi preverjanja prisotnosti novih groženj. Če zaznamo možnost preteče grožnje, je potrebno dodajati nove ali spreminjati obstoječe varnostne kontrole in temu primerno posodobiti varnostno politiko (Hobbs, 1997). Aktivnosti, povezane z varnostjo, moramo zaradi nenehnih sprememb na področju zakonodaje, programske opreme in pogodbenih obveznosti redno spremljati, vrednotiti in testirati.

Upravljavci informacijskih virov morajo prevzeti vodilno vlogo in odgovornost v procesu testiranja poslovnih procesov in preverjanju skladnosti s politiko, kakor tudi vzdrževanje vsebine varnostne politike. Končna dokumentacija varnostne politike mora biti posredovana in na vpogled vsem zaposlenim. Zaposleni pa morajo dokument temeljito pregledati in podpisati izjavo o poznavanju in strinjanju z varnostno politiko.

Dokumentirana varnostna politika zajema obsežno področje varovanja, zato podjetja razvijajo dodatne standarde, priporočila in postopke, ki omogočajo uporabnikom, vodstvu in ostalim zaposlenim jasnejši pristop k vpeljevanju varnostne politike in k uresničevanju ciljev poslovanja.

4.3 Organiziranost varnostne politike

Varnostna politika je lahko napisana kot en sam dokument, lahko pa je razdeljena na več nivojev, od krovnega na najvišjem, taktičnega na srednjem in operativnega na najnižjem nivoju. Ker moja diplomska naloga izhaja iz organizacije, kjer je uporabljen večnivojski način, in so bile ob vzpostavljanju varnostne politike upoštevane smernice standarda BS 7799, se bom osredotočil na večnivojsko obliko varnostne politike.

Z nivoji se doseže prehod od strateških usmeritev in ciljev do konkretnih postopkov in tehnologij, ki se bodo uporabljali za izpolnitev zastavljenih ciljev. Z ločitvijo na nivoje se doseže tudi boljša preglednost nad dokumentacijo. Poleg tega na ta način lahko do različnih nivojev dokumentov dostopajo različni uporabniki.

Slika 3: Večnivojska ureditev varnostne politike

Vir: Rakovec, 2005, str. 32.

Priporočljivo je, da se varnostna politika razdeli na tri nivoje, in sicer (Rakovec, 2005):

- krovna varnostna politika na najvišjem nivoju;
- varnostne politike za posamezna področja (pod politike) na srednjem nivoju in
- delovna navodila, procedure in obrazci na najnižjem nivoju

4.3.1. Krovna varnostna politika

Na najvišjem nivoju je krovna politika, ki predstavlja temeljni dokument za varovanje informacij v podjetju. Osnovni cilj tega dokumenta je pridobivanje podpore in priprava organizacije na izgradnjo celovitega sistema varovanja.

Krovna varnostna politika mora biti potrjena s strani vodstva. V njej morajo biti razvidni namen in vsi cilji, h kateremu stremi. Opredelijo se vloge in odgovornosti zaposlenih in oddelkov. Pripravi in organizira se vsa potrebna dokumentacija. Ker je pričakovano, da bo prihajalo do varnostnih incidentov, se oblikuje postopek prijave varnostnega incidenta, opredelijo pa se tudi sankcije za morebitne kršitelje. Določijo se varnostne politike za posamezna področja. Vse to pa je seveda usklajeno s smernicami standarda BS 7799. Na koncu se določi tudi datum veljavnosti varnostne politike (Rakovec, 2005).

4.3.2. Varnostne politike za posamezna področja

Varnostne politike za posamezna področja so dokumenti srednjega nivoja. V teh dokumentih so podrobneje opisana posamezna področja in sklopi. Naštevam nekaj primerov takih varnostnih politik za posamezna področja (Interni viri ARSKTRP):

- Zagotavljanje fizične varnosti;
- kontrola dostopa do sistema;
- zagotavljanje kontinuitete izvajanja;
- ravnanje z osebnimi podatki;
- ravnanje z osnovno opremo;
- politika dodeljevanja in nadzora dostopov...

4.3.3. Operativna navodila, interni standardi in postopki za delo

Operativna navodila, interne standarde in postopke za delo najdemo na najnižjem nivoju varnostne politike. Ti zelo natančno določajo postopke za posamezna področja (Interni viri ARSKTRP).

- Zahtevek za dostop do računalniškega sistema, namenske programske opreme in podatkov (Priloga 2);
- pravila o upravljanju in varovanju sistemskih gesel;
- pravila o vzdrževanju računalnikov in računalniške opreme;
- pravila o varovanju podatkov na računalniškem sistemu...

4.4. Neprekinjeno poslovanje

Sam informacijski sistem in s tem tudi družba sama mora preživeti tudi takrat, ko se pojavijo naravne ali druge nesreče. V te namene se izdela plan za neprekinjeno poslovanje. Namen tega plana je ugotavljanje in zmanjševanje nevarnosti za nemoteno poslovanje družbe in hitra vzpostavitev ključnih poslovnih aktivnosti po nesrečah. BS 7799, Kodeks varovanja informacij navaja, da mora načrtovanje neprekinjenega poslovanja vključevati ukrepe za ugotavljanje in zmanjševanje nevarnosti.

V planu za neprekinjeno poslovanje morajo biti opredeljene kritične in vitalne poslovne funkcije, ki morajo biti zaščitene pred večjimi nesrečami in katastrofami. Kritičnost poslovnih funkcij je določena na podlagi analize tveganj. Analiza tveganj vključuje po prioriteti razvrščene kritične sisteme v skladu s časovno občutljivostjo, kritičnostjo in neobhodno potrebo za nadaljevanje poslovanja, ki sledi nesreči (Andolšek, Javornik, 2006).

Hitra ponovna vzpostavitev kritičnih poslovnih funkcij preprečuje, da bi prekinitve povzročile katastrofalne posledice za poslovanje. S planiranjem obnove po katastrofi se ne obnovi cela organizacijska struktura, ampak le ključni procesi.

4.4.1. Zbiranje podatkov

Pred začetkom izdelave plana za obnovo se morajo zbrati podatki o poslovnih funkcijah in o zahtevah, ki so povezane s temi funkcijami. Opredeli se tudi medsebojna povezanost poslovnih funkcij. Vodje oddelkov morajo oceniti stroške, ki bi nastali v primeru daljše neuporabnosti sistemov. Vodje organizacijskih enot morajo izvesti popis poslovnih funkcij. Zagotoviti morajo jasen opis podatkov in zapisov poslovnih funkcij za zahteve arhiviranja. Sledi ocena zunanjega vpliva stroškov in ocena kritičnosti. Na koncu pa se ugotovijo odvisnosti med posameznimi funkcijami in drugimi sredstvi.

4.4.2. Analiza tveganj

Analiza tveganj predstavlja formalni pristop za oceno izpostavljenosti družbe. Ugotoviti se morajo, katere katastrofe oziroma nesreče pretijo in kako so le-te povezane z možnimi izgubami. Faza analize tveganja zajema izdelavo seznama kritičnih sistemov, ugotavljanje groženj za te sisteme v obliki naravnih nesreč in izdelavo ocene, kaj za družbo predstavlja nesprejemljivo prekinitev, oziroma maksimalni dopustni čas prekinitve. Upoštevati se mora tudi finančni vidik prekinitve.

Obe fazi pa sta vseeno sekundarnega pomena. Najpomembnejše je, da učinkovito deluje sistem arhiviranja, kajti če enkrat izgubimo podatke, jih izgubimo za vedno. Če ima družba dobro urejeno arhiviranje podatkov, je že na dobri poti pri zagotavljanju neprekinjenega poslovanja.

5. INFORMACIJSKA VARNOSTNA POLITIKA V ARSKTRP

Informacijska varnostna politika v Agenciji Republike Slovenije za kmetijske trge in razvoj podeželja je razvita na podlagi smernic standarda BS 7799. Zahteve po tako organizirani varnostni politiki so prišle s strani Evropske Unije. Samo izvajanje določil politike pa kontrolira letna zunanja revizija.

5.1. Splošno o Agenciji Republike Slovenije za kmetijske trge in razvoj podeželja

Vlada Republike Slovenije je 7.1. 1999 sprejela sklep o ustanovi Agencije Republike Slovenije za kmetijske trge in razvoj podeželja (ARSKTRP) kot organa v sestavi Ministrstva za kmetijstvo, gozdarstvo in prehrano (MKGP). ARSKTRP je bila ustanovljena po evropskem zgledu z namenom izvajanja programov reforme kmetijske politike in izplačevanja sredstev v okviru predpristopnega programa SAPARD (Agencija Republike Slovenije za kmetijske trge in razvoj podeželja, 2007).

Agencija je polno akreditirana za izvajanje najzahtevnejših postopkov pri dodeljevanju finančnih sredstev na področju kmetijstva, živilsko-predelovalne panoge

in razvoja podeželja. ARSKTRP poleg ukrepov neposrednih plačil, ukrepov Programa razvoja podeželja RS 2004-2006, ukrepov kmetijskih trgov, strukturnih ukrepov razvoja podeželja v okviru 3. Prednostne naloge Enotnega programskega dokumenta RS 2004-2006 ter ukrepov za odpravo posledic naravnih nesreč izvaja tudi ukrepa Finančnega instrumenta za usmerjanje ribištva (FIUR, FIFG – Financial Instrument for Fisheries Guidance).

ARSKTRP je zadolžena za preverjanje administrativne in vsebinske ustreznosti prispelih vlog in zahtevkov. Pri tej obravnavi se izvaja vrsta različnih kontrol, na osnovi katerih se obračunajo plačila oziroma se določajo zneski za izplačilo v skladu z nacionalno in evropsko zakonodajo. Skrbi za pravilno in pravočasno izplačevanje odobrenih sredstev končnim prejemnikom ter o tem poroča vladnim in evropskim institucijam (Agencija Republike Slovenije za kmetijske trge in razvoj podeželja, 2007).

Temeljne naloge agencije so (Interni viri ARSKTRP):

- Izvajanje ukrepov kmetijske strukturne politike in politike razvoja podeželja;
- Vzpostavitev in izvajanje integriranega administrativnega in kontrolnega sistema oziroma neposrednih plačil v kmetijstvu (IAKS);
- Izvajanje pomoči in izplačil v primeru naravnih nesreč;
- Izvajanje ukrepov kmetijske tržne cenovne politike, zbiranje podatkov za tržno informacijski sistem za področje mleka, govejega in svinjskega mesa, drobnice, jajc in zelenjave ter vzpostavitev in izvajanje tržno informacijskega sistema (TIS);
- Izvajanje notranje kontrole in notranje revizije.

Pravne podlage za delo ARSKTRP so zakoni, vladne uredbe in izvedbeni podzakonski predpisi (uredbe in pravilniki), ki jih izda minister, ter navodila za delo in priročniki, ki jih za interne potrebe izda predstojnik agencije. Deluje tudi na podlagi zakonodaje in uredb EU ter na podlagi mednarodnih sporazumov. ARSKTRP je v upravnih postopkih prvostopenjski organ pri uveljavljanju podpor ali drugih pravic iz naslova ukrepov (skupne) kmetijske politike.

5.2. Varnostna politika ARSKTRP

Varnostna politika v Agenciji Republike Slovenije za kmetijske trge in razvoj podeželja je organizirana več nivojsko. S tem je omogočeno najbolj učinkovito varovanje informacij. Na vrhu imamo krovno varnostno politiko, na srednjem nivoju so oddelčne varnostne politike, obrazci in navodila pa se nahajajo na najnižjem nivoju. Sam dokument Politika varovanja informacij definira pristop k upravljanju varovanja informacij na ARSKTRP tako, da informacijska sredstva ARSKTRP na primeren način ščiti pred raznovrstnimi notranjimi ali zunanjimi grožnjami, povzročenimi namerno ali nenamerno. Pod grožnjami se razumejo napake, prevare, sabotaže, terorizem, motnje v informacijskem sistemu, kraje, naravne katastrofe, ipd.

5.2.1. Krovna varnostna politika

Krovna politika in njene podrejene politike posameznih področij so razvite s pomočjo vodil standarda SIST ISO/IEC 17799:2003 in SIST BS 7799-2:2003.
Razvoj se je začel leta 2003 in s tem tudi vpeljava varnostne politike (Interni viri ARSKTRP).

Informacije in informacijski sistemi so ključni dejavnik vsakodnevnih aktivnosti. Bistveni del uspeha poslovanja ARSKTRP predstavljajo naslednja tri načela (BS/IEC 17799:2000):

- Zaupnost – zaščita zaupnih in občutljivih informacij pred razkritjem, izgubo poškodbo ali uporabo nepooblaščenih oseb;
- Celovitost – zavarovati točnost in popolnost informacij pred nepooblaščenim spreminjanjem, dodajanjem, brisanjem, narejenim z namenom ali po nesreči;
- Razpoložljivost – zagotoviti, da so informacije na voljo takrat, ko jih potrebujemo.

Do učinkovitega varovanja informacij bo prišlo le s primernim disciplineranim delom zaposlenih. Priti mora do dviga informacijske kulture med zaposlenimi in zavedanja o pomembnosti varovanja informacij. S pravilnim izvajanjem Politike varovanja informacij se ščitijo informacijska sredstva in informacije, ki so shranjene v obliki podatkov na računalnikih, magnetnih trakovih ali drugih izmenljivih medijih, podatki, ki se prenašajo preko omrežij, natisnjeni podatki ali podatki napisani na papirju, podatki poslani po telefaksu, elektronski pošti, disketah ali trakovih, izgovorjeni v pogovoru ali po telefonu.

Izvajanje politike varovanja informacij (Interni viri ARSKTRP):

- Zagotavlja, da so informacije zaščitene pred nepooblaščenim dostopom in na način, ki je primeren njihovi občutljivost, vrednosti in kritičnosti;
- Zagotavlja, da so vse računalniške zmogljivosti, aplikacije, podatki, omrežje in oprema primerno zaščiteni pred izgubo, napačno uporabo ali zlorabo;
- Zagotavlja letni pregled tveganj, katerim so izpostavljena informacijska sredstva ARSKTRP;
- Zagotavlja popravne akcije tam, kjer varnostni incidenti in revizijska poročila kažejo na nezadostno varnost informacij in informacijskih sredstev;
- Zagotavlja, da se izdelajo, vzdržujejo in testirajo načrti za neprekinjeno poslovanje kritičnih poslovnih procesov v primeru katastrof ali velikih odpovedi;
- Zagotavlja, da so vsi uporabniki seznanjeni in podrejeni Krovni politiki varovanja informacij in politikam, ki se navezujejo na njo, ter so seznanjeni in delujejo z navezujočimi priročniki in navodili;
- Zagotavlja, da so vsi uporabniki seznanjeni in delujejo v skladu z navodili ARSKTRP, ki so v skladu z zakonodajo Republike Slovenije;
- Znotraj organizacije ustvarja zavest ljudi, da se morajo ustrezni varnostni ukrepi uvesti kot del učinkovitega delovanja in podpore informacijske varnosti;

- Zagotavlja, da vsi uporabniki razumejo odgovornost glede zaščite zaupnosti in celovitosti podatkov, s katerimi ravnajo;
- Zagotavlja izvajanje izobraževanja in usposabljanja o varovanju informacij za vse stalno ali občasno zaposlene.

Vsi vodje notranjih organizacijskih enot so neposredno odgovorni za vpeljevanje politike na njihovih poslovnih področjih in za upoštevanje politike varovanja informacij pri svojih zaposlenih. Vsi stalno ali občasno zaposleni, kot tudi zunanji partnerji in študentje, so dolžni spoštovati načela Krovne politike varovanja informacij in navezujočih politik na nižjih nivojih. S tem dejstvom morajo biti vsi tudi seznanjeni. Pooblaščenec za varovanje informacij pa je odgovoren za vzpostavitev in vzdrževanje politik varovanja informacij ter za dajanje nasvetov in navodil pri pojavljanju varnostnih incidentov.

Če pride do suma na varnostni incident ali kršitev varovanja informacij, mora biti ta sum posredovan nadrejenemu ali pooblaščencu za varovanje informacij, ki bo svetoval, kakšne korake je potrebno narediti za zmanjšanje nastale škode. Pooblaščenec za varovanje informacij mora redno poročati Varnostnemu forumu o povečanih tveganjih in varnostnih incidentih.

Vsi zaposleni morajo s svojim podpisom potrditi, da so seznanjeni in se tudi strinjajo z vsebino politike varovanja informacij in vsebino podpornih politik na za to namenjenem obrazcu (Priloga 1). Izjavo o politiki varovanja informacij se pregleda letno oz. takrat, ko nastanejo pomembnejše spremembe v informacijski infrastrukturi ali so zabeleženi varnostni incidenti, ki vplivajo na spremembo Krovne politike varovanja informacij.

5.2.2. Varnostne politike za posamezna področja

Varnostna merila za nadzor sredstev in procesov so skladna s postopki ARSKTRP. Izvajanje varnostne politike je potrebno redno kontrolirati in nadzirati. Če se ugotovi, da bi bilo mogoče proces varovanja spremeniti ali izboljšati, odgovorne osebe predlagajo uvedbo sprememb. Za izvajanje in mesečno kontroliranje ter nadziranje je odgovoren vodja Oddelka za dostop do podatkov. Pri pregledih pa izpolni kontrolno listo, ki je sestavni del dokumenta Varnostne politike (Priloga 4).

Področja varnostne politike na ARSKTRP so (interni viri ARSKTRP):

- Zagotavljanje fizične varnosti;
- Kontrola dostopa do sistema;
- Osebna odgovornost;
- Uporaba računalniškega sistema;
- Upravljanje sistema;
- Upravljanje s težavami pri delu z informacijsko tehnologijo;
- Nadzor razvoja sistemov;
- Zagotavljanje kontinuitete izvajanja;
- Ravnanje z osebnimi podatki;

- Ravnanje z osnovnimi sredstvi.

Zagotavljanje fizične varnosti
Fizična varnost je zagotovljena za preprečevanje nepooblaščenega dostopa, škode in motenj v storitvah informacijske tehnologije. Sama informacijska tehnologija se nahaja v varovanih prostorih, do katerih imajo dostop le pooblaščene osebe. Tu so vpeljani varnostni mehanizmi za zagotavljanje fizične varnosti, npr. proti kraji, uničenju ali drugimi nevarnostmi (ogenj, voda, poškodbe zaradi prekinitve električne energije). Dostop zaposlenih do delovnih sredstev ARSKTRP je kontroliran in nadziran.

Kontrola dostopa do sistema
Za identifikacijo uporabnikov in preverjanje uporabniških pravic je vpeljan postopek dodeljevanja uporabniških gesel in pravic ter postopek za redno menjavo uporabniških gesel. Vsi dostopi do sistema in uporaba sistema s strani uporabnikov so kontrolirani in nadzirani. To je še posebej pomembno zaradi nadzora nad morebitnimi nepooblaščenimi dostopi do sistema.

Osebna odgovornost
S postopki varovanja se je potrebno ukvarjati že v času pridobivanja in prerazporejanje zaposlenih v organizaciji zaradi zmanjševanja nevarnosti človeških napak, kraj, prevar ali zlorab naprav. Če se delovno področje zaposlenega spremeni, se preučijo njegove obstoječe pravice dostopa do informacijskega sistema in se po potrebi spremenijo. Vsi zaposleni na ARSKTRP morajo biti seznanjeni s postopkom poročanja o dogodkih, ki so povezani z varnostjo. Zaposleni ne smejo uporabljati programske opreme, ki ni licenčna. Pred samo dodelitvijo pravic za uporabo informacijske tehnologije morajo uporabniki skozi ustrezno izobraževanje.

Uporaba računalniškega sistema
Zaposleni so dolžni spoštovati navodila o uporabi delovnih postaj/programske opreme in se držati navodil o varnosti in zaščiti podatkov ter zaščiti pred vdorom virusov.

Upravljanje sistema

Obsega:

- Postopke za upravljanje sistema, njihovo izvajanje in dokumentiranje;
- namestitev izključno licenčne programske opreme in opreme, ki ni okužena z računalniškimi virusi. Namestitev sme izvajati le pooblaščena oseba v spremstvu Službe za informacijsko upravljanje in tehnologijo (SIUT);
- postopke in programe za ugotavljanje računalniških virusov;
- postopke za shranjevanje, prenos in izločanje podatkov;
- pregledovanje poročil o dostopu do računalniškega sistema;
- evidenco vse strojne in programske opreme.

Upravljanje s težavami pri delu z informacijsko tehnologijo
Vsi postopki za odpravljanje težav in napak, do katerih prihaja pri delu z informacijsko tehnologijo, so določeni in jih je potrebno dokumentirati.

Nadzor razvoja sistemov
Ko se razvija programska oprema, se mora razvojno področje ločiti od testnega in produkcijskega področja. Pri razvoju se je potrebno držati standardov in postopkov za razvoj, nameščanje in testiranje programske opreme. Standardi in postopki morajo biti definirani tako, da razvit sistem ustreza zahtevam uporabnikov ARSKTRP po kakovosti, varnosti in funkcionalnosti. Sistem pa je tudi zaščiten pred nepooblaščenim izvajanjem sprememb.

Zagotavljanje kontinuitete izvajanja
Sem spadajo postopki za varnostno shranjevanje podatkov in hranjenje kopij in jih je potrebno preverjati vsaj enkrat letno.

Ravnanje z osebnimi podatki
Z osebnimi podatki, ki se pojavljajo v informacijskem sistemu, je potrebno ravnati v skladu z veljavno zakonodajo (Zakon o varstvu osebnih podatkov).

Ravnanje z osnovnimi sredstvi
Vsa osnovna sredstva ARSKTRP morajo imeti identifikacijsko številko in morajo biti popisana. V popisu mora biti naveden tudi uporabnik osnovnega sredstva.

5.3. Varnostni forum

Krovna politika varovanja informacij - Izjava vodstva je temelj, na katerem so bile izdelane in sprejete posamezne podporne politike. Te podporne politike se nanašajo na posamezna področja varovanja informacij, kot npr. na dostop uporabnikov do baz podatkov, kreiranje uporabniških pravic in v nekaterih primerih na specifične uporabnike, npr. tiste, ki imajo dostop do ključnih informacij ARSKTRP. Podporne politike morajo biti izdelane na podlagi posvetovanja odgovornih javnih uslužbencev, potrjene in odobrene pa morajo biti s strani **Varnostnega foruma.**

Člane Varnostnega foruma s sklepom imenuje in razrešuje direktor/-ica ARSKTRP. Sam Varnostni forum je sestavljen iz najmanj pet oziroma največ deset članov. Člani Varnostnega foruma izvolijo predsednika, podpredsednika foruma ter strokovnega tajnika.

Člani Varnostnega foruma se morajo udeleževati sej Varnostnega foruma, kjer sodelujejo pri delu ter odločajo o predlaganih sklepih, stališčih in mnenjih. V primeru, da se član trikrat zaporedoma neupravičeno ne udeleži seje Varnostnega foruma, lahko direktor/-ica ARSKTRP takega člana nadomesti z novim članom.

Člani foruma morajo varovati podatke zaupne narave in poslovno tajnost. V posebnih primerih lahko forum k posameznim zadevam povabi strokovnjake za posamezna področja, še posebno takrat, ko je to nujno potrebno za obravnavanje določene zadeve (npr. pravno področje).

Učinkovitost dela Varnostnega foruma se ocenjuje vsako leto. Za doseganje večje učinkovitosti lahko Varnostni forum predlaga tudi spremembe glede sestave foruma.

Namen Varnostnega foruma je (Interni viri ARSKTRP):

- Formalno odobri vpeljavo podpornih politik posameznih področij;
- Odobri posebne vloge in odgovornosti pri varovanju informacij v organizaciji;
- Odobri in podpira pobude za varovanje informacij v celotni organizaciji, npr. program seznanjanja z varovanjem informacij;
- Preučuje napotke za spremembo podpornih politik in jih odobri ali zavrne kot neprimerne;
- Zagotavlja, da se pri spremembah Politike varovanja informacij in podpornih politik upoštevajo tudi vpleteni partnerji, tako zunanji kot notranji;
- Obravnavanje poročil o incidentih in drugih dogodkih, ki so resno vplivali na varovanje informacij, in akcijah, ki so bile narejene za zmanjševanje povzročene škode;
- Pregleduje oceno tveganja za grožnje, povezane z varnostjo informacij in predlaga kontrole;
- Pregleduje revizorska poročila in predloge;
- Nadzira razvoj strategije varovanja informacij na ARSKTRP;
- Spodbuja razumevanje poslovnega pomena varovanja informacij v organizaciji;
- Ažurno informira vodstvo ARSKTRP o razvoju in napredku sistema varovanja informacij, pa tudi o resnih kršitvah politike varovanja informacij.

Poleg ustnega in pisnega obveščanja so za sprejemanje prijav o varnostnih incidentih na ARSKTRP odprli elektronski poštni predal (varinfo.aktrp@gov.si), kjer lahko zaposleni in stranke v postopku prijavljajo morebitne varnostne incidente ali sume kršitve varovanja informacij. Pooblaščenec za varovanje informacij pa mora pregledovati vsebino poštnega predala, nuditi pomoč in svetovanje pri odpravi varnostnih incidentov ter na podlagi tega izdelati tedensko poročilo.

Sejo Varnostnega foruma skliče njegov predsednik. Glede na velikost in stopnjo tehnološkega razvoja Agencije so se člani Varnostnega foruma dolžni sestajati vsake 3 mesece ali po potrebi pogosteje. V tem primeru sestanek skliče predsednik Varnostnega foruma na svojo pobudo ali na pobudo katerega koli izmed članov.

6. ANALIZA VARNOSTNE POLITIKE ARSKTRP

Pri analizi se bom v prvem delu osredotočil na področja varnostne politike in na to, kako je v ARSKTRP za ta posamezna področja poskrbljeno. Opisal bom, kako poteka administracija uporabnikov, ker se v tej organizaciji s tem ukvarjam in poznam tudi vse probleme, ki pri tem nastajajo. Prikazal bom tudi, kako se ravna z zaposlenimi, kako se usposabljajo, kakšni so postopki pri novih zaposlenih, kako se ravna v primeru incidentov ali okvar. Opisal bom, kakšno stanje je bilo pred uvedbo standarda, kakšno je sedaj po uvedbi, do kakšnih težav je prihajalo pri uvajanju

uporabnikov in tudi ostala področja, ki bi bila lahko vsekakor boljša. Naštevam tudi predloge kot potencialne možnosti z namenom, da se ta področja optimizirajo.

6.1. Analiza varnostne politike po področjih

Varnostna politika na Agenciji Republike Slovenije za kmetijske trge in razvoj podeželja je organizirana na več nivojih. Tukaj se bom osredotočil na politike po področjih. Izhajal bom iz področij varovanja, ki sem jih navedel in jih kratko opredelil že zgoraj: zagotavljanje fizične varnosti, kontrola dostopa do sistema, osebna odgovornost, uporaba računalniškega sistema, upravljanje sistema, upravljanje s težavami pri delu z informacijsko tehnologijo, nadzor razvoja sistemov, zagotavljanje kontinuitete izvajanja, ravnanje z osebnimi podatki, ravnanje z osnovnimi sredstvi.

6.1.1. Zagotavljanje fizične varnosti

Namen zagotavljanja fizične varnosti je preprečevanje nepooblaščenega dostopa, škode in omejitev v delovanju informacijskega sistema. Za boj proti virusom je na ARSKTRP uporabljen antivirusni program Sophos. Ob morebitnem napadu virusa je obveščen tako uporabnik kot tudi servis na Službi za informacijsko upravljanje in tehnologijo. Sam Sophos se je na področju varovanja proti virusom izkazal za zelo učinkovitega. Edina slabost pa je v tem, ker je na ARSKTRP precej starejših računalnikov in ta program porabi velik delež delovnega spomina, kar pa te računalnike upočasni in s tem podaljšuje delo.

Vsa informacijska tehnologija se nahaja v varovanih prostorih, do katerih imajo le pooblaščeni. Prostori so varovani s kamerami in alarmom, ki preprečujejo nepooblaščeni vstop. Sama notranjost sistemskih prostorov je klimatizirana, saj se edino tako lahko zagotovi potrebna temperatura za optimalno delovanje strojne opreme. Sami temperaturni senzorji so tudi povezani na alarm, kajti če se temperatura pretirano poveča, se poveča tudi verjetnost za nastanek požara. V zadnjem letu pa so vgradili v sistemsko sobo tudi vodne senzorje, ki opozarjajo na morebitno poplavo v prostoru. Zaradi zahtev revizije se je letos vgradil tudi nov požarni zid, ki varuje celoten informacijski sistem pred nepooblaščenimi vdori.

6.1.2. Kontrola dostopa do sistema

Za identifikacijo uporabnikov in preverjanje uporabniških pravic je vpeljan postopek dodeljevanja uporabniških gesel in pravic ter postopek za redno menjavo uporabniških gesel. Vse to je omogočeno preko Novella. Več o sami administraciji bom povedal v nadaljevanju. Vsaka prijava v sistem se zabeleži, kar tudi omogoča nadzor nad morebitnimi nepooblaščenimi vdori v sistem.

Razni obiskovalci se ne smejo gibati brez spremstva po območju Službe za informacijsko upravljanje in tehnologijo. Pri recepciji počakajo na spremstvo, navadno je to nekdo iz Službe za informacijsko upravljanje in tehnologijo (SIUT). Le tako imajo obiskovalci vstop v prostore agencije.

6.1.3. Osebna odgovornost

Vsi uporabniki informacijskega sistema na ARSKTRP se zavežejo s svojim podpisom na izjavi o varnostni politiki (priloga 1), da bodo spoštovali določila, ki jih zahteva varnostna politika. Če zaposleni ugotovijo kak varnostni incident, morajo informacijo o tem posredovati pooblaščencu za informacijsko varnost. Za tako poročanje je namenjen posebni elektronski poštni predal. Vendar pa sam opažam, da ta sistem trenutno ne deluje najbolje, še posebno ne na področju manjših varnostnih incidentov. Zaposleni namreč manjših incidentov sploh ne opazijo ali pa jih zatajijo z namenom, da bi delo potekalo bolj tekoče.

Zaposleni ne smejo uporabljati programske opreme, ki ni licenčna. Problem je v tem, da so vse te licence od operacijskih sistemov na posameznem računalniku nepravilno evidentirane in jih je zato skoraj nemogoče najti. Pojavljajo pa se tudi posamezni uporabniki, ki licenčne programske opreme nimajo. Navadno so to informatiki, ki si kak program, če ga že potrebujejo, največkrat posnamejo iz interneta.

Preden začnejo uporabniki (novi zaposleni) uporabljati informacijski sistem, morajo skozi izobraževanje. Vendar pa sem opazil, da je to izobraževanje pomanjkljivo, saj uporabniki večkrat sprašujejo najosnovnejše stvari in tudi njihova seznanjenost s samo varnostno politiko je na nezavidljivem nivoju.

6.1.4. Uporaba računalniškega sistema

Zaposleni se morajo pri uporabi računalniškega sistema, to je računalniške in programske opreme, držati za to določenih navodil. Varovati morajo vse podatke, s katerimi upravljajo. Ne smejo obiskovati spletnih strani, na katerih je večja možnost okužbe z računalniškim virusom. Sama navodila za učinkovito uporabo računalniškega sistema uporabniki najdejo v mapi, ki je dostopna vsem zaposlenim. Na ta način naj bi se zagotovilo, da navodila poznajo vsi, ki jih potrebujejo za svoje delo. V sami praksi ARSKTRP se je izkazalo, da se na splošno uporabniki premalo zavedajo groženj. To spet kaže na potrebo po nekakšnem organiziranem izobraževanju zaposlenih s področja varovanja informacij.

6.1.5. Upravljanje sistema

Za upravljanje sistema je zadolžena Služba za informacijsko upravljanje in tehnologijo (SIUT). Vsa programska oprema, ki se namešča, mora biti licenčna. Namestitev izvede pooblaščena oseba in vedno v spremstvu zaposlenega iz SIUT-a.

V tej točki so definirani postopki in programi za ugotavljanje računalniških virusov. Kot sem omenil, na agenciji uporabljajo programski paket Sophos. Protivirusni program se osvežuje najmanj enkrat mesečno. Če pride do okužbe z virusom, se okužena datoteka preseli v karanteno in s to datoteko je onemogočeno delo, dokler se virus ne odpravi. Podatki se shranjujejo, prenašajo in izločajo po pravilniku, ki je viden vsem.

Služba za informacijsko upravljanje in tehnologijo skrbi za redno pregledovanje poročil o dostopu do računalniškega sistema ARSKTRP in seveda vodi evidenco vse strojne opreme na agenciji. To evidenco pa je v praksi izredno težko vzdrževati. Na ARSKTRP je zaposlenih več kot tristo ljudi (zaposleni in študenje) in velikokrat se selijo iz ene pisarne v drugo. Po pravilih bi morali obvestiti SIUT o selitvi, saj se zaposleni navadno seli s svojo opremo, vendar velikokrat temu ni tako. Zato se evidenca ne posodablja tako hitro, kot se dogajajo te interne selitve. Že zgoraj sem omenil, da je evidenca programske opreme na slabem nivoju, vendar pa naj povem, da so se v zadnjem času na tem področju zgodili nekateri premiki, ki so posledica negativnega mnenja revizije na tem področju.

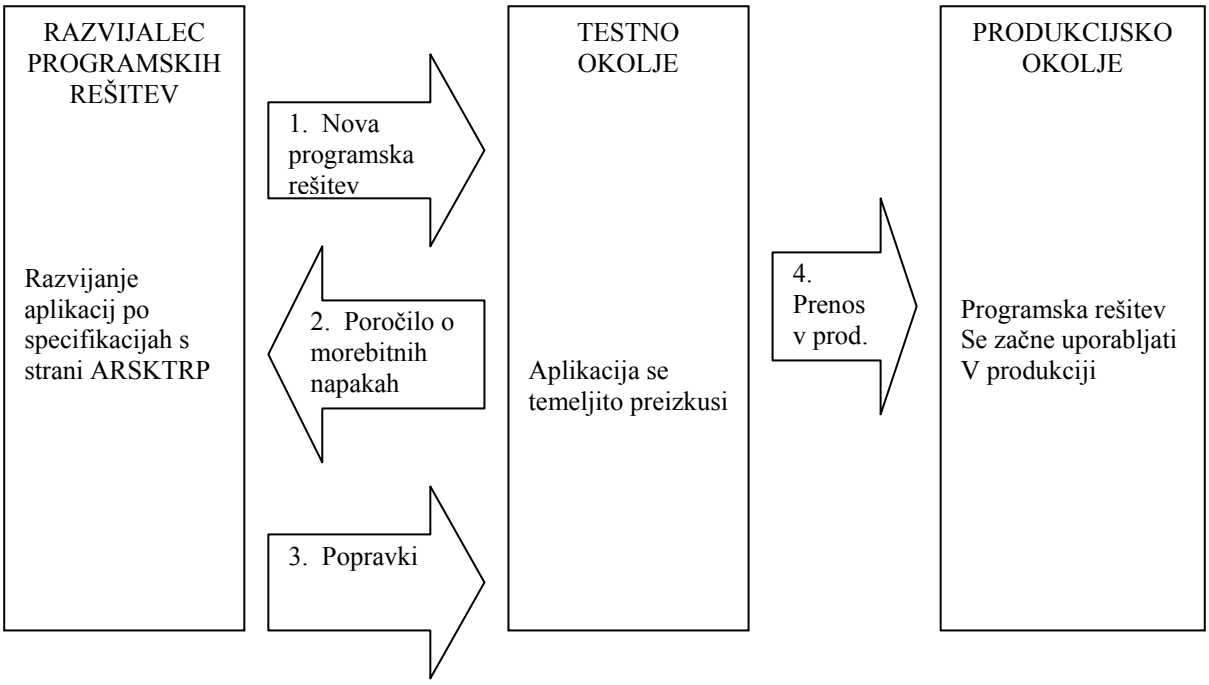
6.1.6. Upravljanje s težavami pri delu z informacijsko tehnologijo

Sami postopki za upravljanje s težavami pri delu z informacijsko tehnologijo so določeni, vendar pa se v praksi niti ne izvajajo. Sam opažam, da je ta postavka tu samo zato, da je varnostna politika v popolnosti skladna s standardom BS 7799. V resnici pa je temu sklopu podana premajhna pozornost.

6.1.7. Nadzor razvoja sistemov

ARSKTRP zaradi značilnosti svojega dela ne more preprosto kupiti že izdelane programske opreme, zato je prisiljena na razvoj lastnega sistema. Do samega razvijanja programskih rešitev pa prihaja s sodelovanjem z zunanjimi razvijalci. Ti zunanji razvijalci se izbirajo s pomočjo javnega razpisa.

Slika 4: Postopek uvajanja programskih rešitev



Vir: Lastno delo, 2007.

Razvojno okolje je na agenciji razdeljeno na testno in na produkcijsko področje. Programske rešitve za ARSKTRP razvijajo zunanji sodelavci. Popolnoma nova programska rešitev ali le njena posodobitev se najprej naloži na testno okolje, kjer se tudi preizkusi. Morebitne napake v aplikaciji se sporočijo razvijalcem in tudi vodstvu ARSKTRP. Naložijo se popravki in zopet sledi preizkus. Ko aplikacija opravi vse potrebne teste, se izda pisni zahtevek za namestitev v produkcijsko okolje.

6.1.8. Zagotavljanje kontinuitete izvajanja

Za zagotavljanje kontinuitete izvajanja ali neprekinjenega poslovanja ima ARSKTRP izdelan izčrpen načrt. V njem najdemo vse postopke, ki morajo biti izvedeni, da bo kontinuiteta čim bolj zagotovljena. Vsebuje tudi razne ukrepe za primere, ko pride do raznih prekinitev v poslovanju, ki so posledica napadov, napak ali naravnih nesreč.

Čez noč se izvaja proces arhiviranja podatkov in izdelave rezervnih kopij (ang. backup). Zjutraj prideta dva varnostnika po kasete, na katerih so shranjene rezervne kopije. Te se nato prepeljejo na varno lokacijo. Pogoj za varno lokacijo je to, da je leta locirana na drugem potresnem območju.

6.1.9. Ravnanje z osebnimi podatki

Z vsemi osebnimi podatki, ki se na kakršenkoli način pojavljajo v informacijskem sistemu, se ravna v skladu z Zakonom o varstvu osebnih podatkov. Na tem področju se ARSKTRP obnaša popolnoma v skladu z zakonom.

6.1.10 Ravnanje z osnovnimi sredstvi

Vsa osnovna sredstva na ARSKTRP imajo identifikacijsko številko. Vsako leto se izvede popis osnovnih sredstev, v katerem se tudi navede uporabnik posameznega osnovnega sredstva. Za popis informacijskih sredstev skrbi Služba za informacijsko upravljanje in tehnologijo. Ta tudi vodi evidenco teh sredstev. Največkrat se prav pri popisu pokažejo nepravilnosti v tej evidenci zaradi problemov, ki sem jih že omenil že zgoraj.

Sama področja varnostne politike so skoraj v popolnosti skladna z zahtevami, ki jih narekuje standard BS 7799. Seveda so tudi manjša odstopanja, saj gre za ogromno organizacijo, ki je v dokaj kratkem času uvedla nov sistem varovanja informacij. V skladnost jih sili redna letna revizija in njene zahteve, ki morajo biti izpolnjene do zahtevanih datumov.

6.2. Administracija uporabniških gesel

Prikazal bom sam postopek administracije uporabniških gesel, ker je bilo to področje največkrat na udaru revizije in tudi zato, ker sem kot skrbnik teh aplikacij na lastni

koži opazil slabosti in prednosti sistema. Opisal bom, kako je potekalo to dodeljevanje pravic v preteklosti in kako poteka to v sedanjosti.

6.2.1. Postopek za pridobivanje uporabniških pravic v preteklosti

V preteklosti je bil postopek za pridobitev uporabniških pravic zelo dolgotrajen in posledica tega procesa je bil kup najmanj dvajsetih strani, na katerih je bilo razvidno, katere pravice bo imel uporabnik. Postopek se je začel tako, da je uporabnik izdal zahtevek za pridobitev določenih pravic na raznih aplikacijah, ali pa mu ga je izdal njegov nadrejeni. Nadrejeni je ta zahtevek potrdil s svojim podpisom. Sam zahtevek je šel potem do kadrovske službe, ki ga je potrdila s svojim pečatom in s svojim podpisom, da je uporabnik dejansko zaposlen na agenciji. Naslednja postaja je bila pisarna generalnega direktorja, ki je s svojim podpisom in pečatom odobril zahtevek. Nazadnje je zahtevek pristal pri skrbniku aplikacij. Tukaj vidimo, da gre za tipičen primer večnivojskega potrjevanja. Možnosti za zlorabo so majhne, vendar pa taka varnost terja svoj davek. Kot sem že prej omenil je sam postopek zelo dolgotrajen in zelo obsežen po papirologiji. Postopek traja vsaj dva do tri dni, kar je za današnje čase in tehnologijo veliko predolgo.

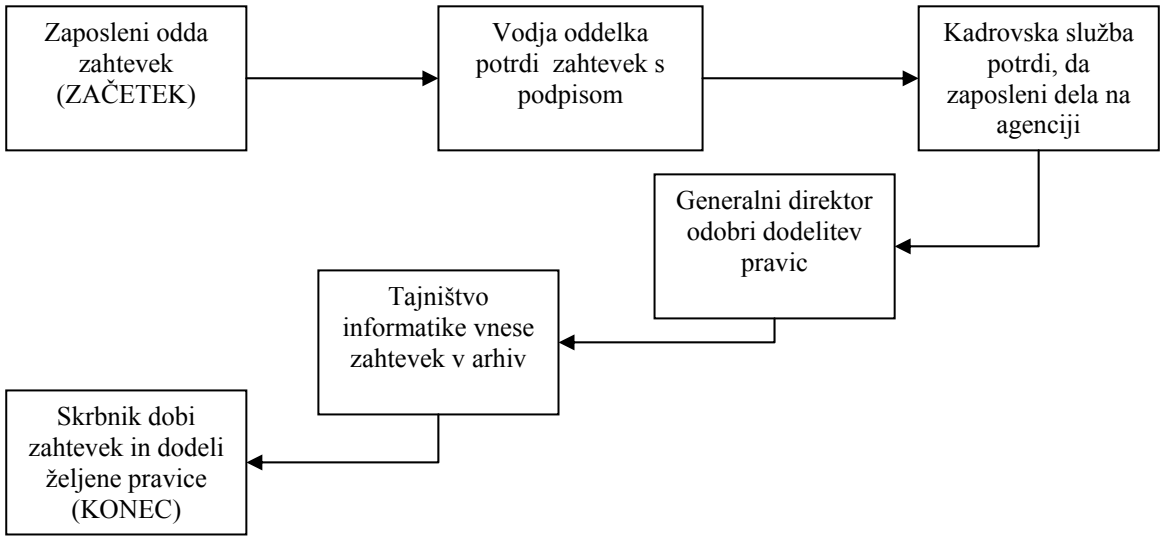
Aplikacije so nastavljene tako, da si morajo uporabniki vsakih 30 dni zamenjati geslo, ker tako narekuje tudi sam standard BS 7799. Če v tem času geslo ni spremenjeno, se nosilec pravic (uporabnik) samodejno zaklene. Do zaklepa pa pride tudi v primeru , če je geslo trikrat napačno vpisano. Na tem mestu spet pride na vrsto skrbnik aplikacij. V preteklosti je uporabnik z zaklenjenim geslom poklical po telefonu skrbnika aplikacij in ta je potem odklenil zaklenjeno geslo. Ta način odklepanja preko telefona se je kasneje izkazal za nepraktičnega z vsaj dveh vidikov. Prvi vidik je ta, da ni bilo vidne nobene evidence, koliko uporabnikom se je bilo geslo zaklenjeno ter koliko dela s tem je imel sam administrator. Na prvi pogled je bilo videti, kot da skrbnik aplikacij nima dela, bilo pa je ravno nasprotno, saj je vsaj deset uporabnikov dnevno kontaktiralo skrbnika aplikacij v zvezi z zaklenjenim geslom. Drugi vidik pa je bil ta, da je moral skrbnik aplikacij pustiti vse svoje delo, če je dobil klic, in odkleniti zaklenjena gesla.

Vse to se je rešilo s tem, da so uporabniki poslali elektronsko pošto o zaklepu gesla na servis ARSKTRP. Na ta način so se uporabniki s težavo privadili. Še vedno so prihajali telefonski klici zaradi odklepa gesel uporabnikov. Odklepanje zaklenjenih gesel uporabnikov ni bilo dovoljeno preko telefona in na vsako opozorilo ob klicu, da morajo poslati elektronsko pošto, je prišlo do negodovanja in očitkov, da se s tem uporabnike po nepotrebnem obremenjuje in da se jim s tem, ko morajo pošiljati elektronsko pošto povzroča le dodatno delo. Sčasoma so se prilagodili na ta način dela. Največ problemov je bilo s strani starejših zaposlenih, saj so se s to novostjo podrli določeni utečeni postopki. Vendar tudi ta način ni bil brez napak. Tak sistem ni omogočal nadzora s strani nadrejenih, kako se rešujejo ti zahtevki. Podaljšali so se odzivni časi. V samih zahtevkih pa ni bila definirana vrsta napake in uporabniško ime uporabnika.

Sistem preprosto ni omogočal celovitega spremljanja naročil in zahtevkov, s tem pa je bilo onemogočeno tudi spremljanje učinkovitosti te podporne službe. Velik problem so predstavljale tudi zahteve uporabnikov za dodelitev določenih pravic, kar preko elektronske pošte. Zelo težko jim je bilo namreč dopovedati, da varnostna politika

narekuje to, da mora biti zahtevek za dodelitev pravice oddan na za to določenem pisnem zahtevku (priloga 3) z vsemi potrebnimi podpisi in žigi. Vsa ta dejstva kažejo na to, da kljub seznanjenosti z varnostno politiko le-te niso dovolj dobro poznali. Načela varnostne politike so uporabniki videli bolj kot oviro in ne kot nekaj, kar pomaga vsem zaposlenim in seveda tudi strankam, s katerimi ARSKTRP sodeluje. Vsi ti dejavniki pa so bili dober pokazatelj, da je potrebno te postopke temeljito prenoviti.

Slika 5: Slika procesa pridobivanja uporabniških pravic



Vir: Lastno delo, 2007.

6.2.2. Postopek za pridobivanje uporabniških pravic v sedanjosti

V današnjem času se postopek niti ni veliko spremenil, le računalniška tehnologija je vse avtomatizirala, bistveno skrajšala čas postopka in odpravila ogromne količine papirja. Postopek se začne tako kot prej, torej ko uporabnik odda zahtevek za dodelitev pravic, vendar pa je razlika v tem, da se ta zahtevek odda v elektronski obliki na za to predpisanem obrazcu. Ta zahtevek uporabnik potem preko elektronske pošte pošlje svojemu nadrejenemu, ki s svojim elektronskim podpisom potrdi zahtevek. Zahtevek nato odide v kadrovsko službo in na koncu seveda do generalnega direktorja. Vsi potrjujejo z elektronskim podpisom. Sam postopek se je skrajšal na maksimalno en dan. Za evidenco o zaposlenih ne potrebujemo več gore papirjev in arhivov, ampak je vse evidentirano elektronsko.

Spremembe so se pojavile tudi na področju odklepanja zaklenjenih gesel uporabnikov ter odpravljanju raznih napak na računalnikih. Izdelan je bil namreč elektronski obrazec, na katerega se napiše, katera aplikacija je zaklenjena, kakšno je

uporabniško ime uporabnika, torej vse podatke, ki jih skrbnik aplikacij potrebuje, da odklene geslo zaklenjenega uporabnika na pravi aplikaciji. V preteklosti je skrbnik aplkacij namreč skoraj na slepo ugibal uporabniško ime. Takrat tudi ni bilo nobenih pravil za tvorjenje posameznega uporabniškega imena, tako da je vsak administrator imel svoj način tvorjenja le-tega. Nadrejenim je bil omogočen nadzor nad tem, kakšni zahtevki prihajajo na servis, skrajšal se je tudi odzivni čas in sam čas izvedbe naloge. S to obliko se je uvedel celovit sistem spremljanja naročil in zahtevkov; nadrejeni so lahko spremljali učinkovitost samega servisa in s tem odkrili ozka grla in tako sprožili postopke, ki so te nepravilnosti lahko odpravile.

Pri samem uvajanju elektronske oblike je pri uporabnikih prihajalo do nasprotovanja novostim, kar je skoraj samoumnevno, saj se skoraj vsi upiramo spremembam. Pokazati smo jim morali, da so te spremembe nujne in da bojo slej ko prej prinesle nekatere prednosti. Do največjih težav je prihajalo pri starejših zaposlenih, saj se v povprečju še težje privadijo na novosti. Te spremembe so nekateri uporabniki jemali zelo osebno in so se pritoževali, kot da gre za kakšno zaroto proti njim. Bilo je potrebno ogromno dela v prepričevanju uporabnikov, da so ti postopki tudi v njihovo dobro. V roku enega meseca so uporabniki končno začeli spoznavati, da so spremembe prinesle ker nekaj prednosti med katerimi je najočitnejša krajša poraba časa za dodelitev pravic.

Osebno vidim problem v tem, da ni bilo nikakršnega posebnega izobraževanja o tem, kakšne bodo spremembe na področju dodeljevanja pravic. Še večji problem pa je ta, da uporabniki niso bili seznanjeni s tem, kaj bojo te spremembe prinesle. Na podlagi te seznanjenosti bi se lažje spopadali s privajanjem na nove postopke. V tem primeru je prišlo tudi do manjšega razkola s standardom BS 7799, saj bi po standardu morali detajlno poučiti uporabnike o spremembah na področju varnostne politike.

6.3. Ravnanje z zaposlenimi

Kot sem že prej omenil mora biti vsak zaposleni, na novo zaposleni in tudi vsak študent seznanjen z vsebino varnostne politike. Tako namreč narekuje tudi sam standard BS 7799, ki je osnova za prenovo informacijskega sistema v Agenciji Republike Slovenije za kmetijske trge in razvoj podeželja. Vsak zaposleni podpiše izjavo (Priloga 1) o tem, da je seznanjen z varnostno politiko, in da bo spoštoval zahteve le-te.

Da bi se še dodatno zmanjšala možnost zlorabe, se je v ARSKTRP uvedla obvezna uporaba spletnega elektronskega osebnega podpisa SIGOV-CA, ki ga izdaja Ministrstvo za javno upravo. Za vsakega zaposlenega smo morali zbrati podatke (ime, priimek, naslov elektronske pošte, davčna številka), da smo lahko sprožili postopek za pridobitev tega certifikata. S tem se je otežil sam nepooblaščen dostop do aplikacij ali celo dostop do službene elektronske pošte. Vse programske rešitve smo namreč prilagodili temu certifikatu, tako da ni mogoče dostopati brez pametne kartice in gesla uporabnika. Novi zaposleni mora sedaj podpisati izjavo o seznanjenosti z varnostno politiko in oddati potrebne podatke za pridobitev SIGOV-CA certifikata (Priloga 5).

6.4. Ravnanje z varnostnimi incidenti

Do manjših varnostnih incidentov, kot so puščanje uporabniških imen in gesel, prilepljenih na ekranih računalnikov, puščanje odprtih vrat, skozi katera je mogoč vstop le s kartico, prihaja vsakodnevno. Glede takih dejanj so zaposleni le redko kdaj opozorjeni in v tem vidim velik problem. Taka ravnanja namreč pomenijo nespoštovanje določil varnostne politike in lahko kasneje pripeljejo do večjih varnostnih incidentov.

Nadrejeni so obveščeni le o večjih varnostnih incidentih, kot so ne delovanje alarma v sistemski sobi, ne delovanje klime v sistemskih prostorih, ti pa kasneje o tem poročajo pooblaščencu za varnost. Vsi ti varnostni incidenti se obravnavajo na Varnostnemu forumu, ki naj bi se odvijal vsake tri mesece.

Problemi so tudi v tem, da se uporabniki velikokrat ne zavedajo pomembnosti varovanja informacij. To se najbolj vidi v primerih, ko se ti podatki natisnejo na papir. Ti dokumenti navadno čakajo na tiskalnikih in se nanje velikokrat kar pozabi. Ker pa ARSKTRP upravlja z ogromno količino osebnih podatkov, lahko to predstavlja veliko večji problem, kot se zdi na prvi pogled. Na te napake običajno opozarja pooblaščenec za varnost preko elektronske pošte. Nekateri uporabniki teh opozoril ne upoštevajo v zadostni meri. Menim, da bi morali biti v ARSKTRP na tem področju bolj odločni in strogi. Odviti bi se morala predavanja na temo o dvigu zavesti o potrebnosti varovanja informacij.

Osebno sem naletel tudi na problem prijavljanja uporabnikov na tuja uporabniška imena. Do tega pride, ker mora nek zaposleni narediti določeno stvar, za katero nima potrebnih uporabniških pravic. Problem je tudi v dolgem postopku za dodelitev pravic, ki je bil aktualen v preteklosti. Preden bi zaposleni dobil zahtevane pravice, bi rok za omenjeno delo že potekel. Na ta problem sem opozoril tudi nadrejene, vendar so mi odvrnili, da je to nemogoče nadzorovati. Dobil pa sem navodilo, da lahko odklenem zaklenjeno geslo uporabnika, le če mi uporabnik osebno pošlje elektronsko pošto, da je njegovo geslo zaklenjeno. Na ta način se je zmanjšalo število prispelih zahtevkov za odklepanje, kajti v preteklosti se je dogajalo tudi to, da je drug uporabnik spremenil geslo in tako se je geslo le-temu kasneje tudi zaklenilo. Tudi tem primeru bi bilo koristno izvesti usposabljanje ali dodatno izobraževanje za zaposlene.

Do večjih varnostnih incidentov prihaja le redko, vendar pa bi morali dati večji poudarek tem manjšim incidentom, saj bi se na tak način dvignila informacijska kultura in samo spoštovanje do varovanja informacij.

6.5. Ostala področja varovanja informacij

Nekaterih področij ne moremo umestiti direktno v samo varnostno politiko, vendar so vredna omembe. Prikazal bom pozitivne in negativne lastnosti ostalih področij varovanja informacij. V tem razdelku bo govora o delovanju varnostnega foruma, o

uvedbi novega načina izmenjevanja podatkov z zunajimi sodelavci in nekaj besed o sami reviziji varovanja informacij.

Tabela 1: Ostala področja varovanja informacij na ARSKTRP

Področja	**Pozitivne lastnosti**	**Negativne lastnosti**
Delovanje varnostnega foruma	Z ustanovitvijo so se upoštevala priporočila standarda BS 7799	Neredno delovanje in sestajanje varnostnega foruma
Izmenjava podatkov z zunanjimi sodelavci	Uvedba varnega načina izmenjave podatkov s pomočjo elektronskega podpisa	Zamudno uvajanje elektronskega podpisa s strani zunanjih sodelavcev
Revizija varovanja informacij na ARSKTRP	Področje varnosti in pridobivanja novih sodelavcev,....	Zagotavljanje procesa neprekinjenega poslovanja,....

Vir: Lastno delo, 2007.

6.5.1. Delovanje Varnostnega foruma

V skladu s standardom BS 7799 je ARSKTRP ustanovila telo za upravljanje varovanja informacij – Varnostni forum. Sestanki Varnostnega foruma bi se morali izvajati vsake tri mesece, vendar temu ni tako, saj se zgodijo taki sestanki na ARSKTRP le enkrat letno. Gre za razhajanje s smernicami, ki si jih je agencija zastavila. Menim, da bi morali sklicevati sestanke Varnostnega foruma vsake tri mesece in s tem dati pomen Varnostnemu forumu, ki si ga zasluži. Potrebno bi bilo tudi obravnavati varnostne incidente in sprejemati odločitve, ki naj bi varnost informacij dvigala.

ARSKTRP ima tudi svojo službo za notranjo revizijo, ki med drugim nadzoruje tudi to, kako se izvaja sama varnostna politika. Po pogovoru z varnostnim inženirjem smo ugotovili, da služba notranje revizije ne poroča o relevantnih ugotovitvah s področja informacijske tehnologije Varnostnemu forumu agencije in zato sam Varnostni forum ne more izvajati nalog, za katere je zadolžen. Poslovodstvo bi moralo na tem področju sprejeti potrebne ukrepe, da se uredijo zadeve med službo za notranjo revizijo in samim Varnostnim forumom, saj se bo edino na tak način na forumu sprejemalo ustrezne ukrepe, ki bodo odpravili ugotovljena odstopanja od sprejetih standardov. Brez tega sodelovanja je forum kot takšen popolnoma brez smisla.

6.5.2. Izmenjava podatkov z zunanjimi sodelavci

Prišlo je tudi do sprememb na področju sodelovanja z zunanjimi sodelavci. Agencija Republike Slovenije za kmetijske trge in razvoj podeželja namreč sodeluje z različnimi organizacijami in med njimi so tudi banke. Do sedaj je potekala izmenjava

podatkov preko navadne pošte ali preko elektronske pošte. Agencija je pošiljala zgoščenke s podatki o izplačilih subvencij določenim kmetom preko navadne pošte na banko ali preko elektronske pošte. Pojavil se je problem, saj so bili ti podatki zapisani na način, ki je vsakemu, ki bi utegnil prestreči to pošiljko, omogočal neomejen vpogled. Prestrezanje elektronske pošte pa v današnjih časih ne predstavlja zahtevne naloge.

Na ta problem je opozorila tudi revizija. Sprožil se je postopek, ki je omogočil zaščito teh podatkov. Tega so se v agenciji lotili tako, da so se morali vsi izhodni podatki kriptirati. To pa se naredi s pomočjo SIGOV-CA certifikatov, to je z elektronskim podpisom. Na tak način delovanja so seveda morali pripraviti tudi zaposlene. Na srečo je to sovpadalo z obdobjem, ko so se naročali SIGOV-CA certifikati za vse zaposlene.

Sam postopek kriptiranja je zelo preprost. Uporabnik zakrpitira datoteko z desnim klikom na miški in tam tudi izbere prejemnika. Le na ta način bo lahko prejemnik odprl datoteko, ki mu je namenjena. Uporabnik, to je največkrat banka, pa mora imeti tudi elektronski podpis, certifikat se imenuje SIGEN-CA. Sama agencija je nekaj mesecev, preden se je ta postopek začel uporabljati, tudi opozorila vse zunanje partnerje, da morajo pridobiti ustrezne certifikate, da bojo lahko uporabljali kriptirane podatke. Kljub vnaprejšnjemu opozorilu je vseeno prišlo do problemov, saj nekateri partnerji niso pravočasno pridobili teh certifikatov.

Po mojem mnenju je v tem primeru ARSKTRP pravilno izpeljala cel postopek, saj je na nov način delovanja pripravila svoje zaposlene in je na to novost pravočasno opozorila zunanje sodelavce. Na dejstvo, ali so se zunanji partnerji tega držali, pa agencija dejansko ni imela vpliva.

6.6. Revizija varovanja informacij na ARSKTRP

Skladno z letnim načrtom dela Urada Republike Slovenije za nadzor proračuna je bila v času od maja do oktobra 2006 izvedena revizija izvedenih ukrepov na področju varovanja informacijskih sistemov na Agenciji Republike Slovenije za kmetijske trge in razvoj podeželja.

Revizija je preverjala, kakšno je stanje na raznih področjih varovanja informacij in podala oceno o tem stanju. Samo ocenjevanje stanja je potekalo leta 2005. Kasneje je podala priporočila, ki naj bi jih agencija izpolnila. V letu 2006 pa je revizija razodela, kako so se spoštovala ta priporočila. Revizorji so ocenjevali z ocenami od 1 do 5, kjer 1 pomeni najslabšo oceno, 5 pa najboljšo. Povprečna ocena vseh ocenjevanjih področij je bila 4, kar je bil tudi cilj ARSKTRP.

Ker ne smem prikazati rezultatov celotne revizije, bom samo opisal najboljše področje in področje, kjer se agencija ni dosledno držala priporočil revizije. Najslabšo oceno je agencija dobila pri upoštevanju priporočil na področju zagotavljanja neprekinjenega poslovanja in zaščite kritičnih poslovnih procesov pred večjimi

okvarami ali nesrečami. Vendar pa lahko povem, da se je na tem področju v času po reviziji veliko naredilo. Vendar pa so varnostni incidenti vseeno prepogosti. Do teh varnostnih incidentov prihaja tudi zaradi trenutne zakonodaje na področju javnih razpisov. En primer je tak, da klime v sistemskih prostorih ne delujejo optimalno in so potrebne popravila. Ker se izbira najugodnejši izvajalec popravil, pa čeprav gre samo za nekaj evrov razlike, v tem času ARSKTRP tvega pregrevanje sistemske sobe in s tem odpoved delovanja strojne opreme. Že kar nekajkrat, se je temperatura nevarno dvignila in s tem ogrozila vse shranjene podatke na diskih v sistemski sobi. Najboljšo oceno pa je agencija dobila na področju varnosti pri opredelitvi dela in pri pridobivanju novih sodelavcev.

7. SKLEP

Informacije, ki jih podjetja uporabljajo, morajo biti točne, zanesljive in pravočasne. Take informacije pa zagotavlja le dobro urejeno varovanje informacij. Ena od možnosti, kako urediti dobro varovanje informacij, je tudi naslanjanje na svetovno priznane standarde. Eden od takih je definitivno varnostni standard BS7799. Vendar je kljub temu, da ne odkrivamo ničesar novega in se le držimo smernic, ki nam jih je zadal standard, uvajanje učinkovitega varovanja informacij dolg in zapleten proces. Na potek in potrebnost sprememb je potrebno opozoriti in pripraviti vse uporabnike informacijskega sistema.

Zahtevnosti uvajanja učinkovitega varovanja informacij so se zavedali tudi na Agenciji Republike Slovenije za kmetijske trge in razvoj podeželja. Dela so se lotili na sistematičen način, vendar pa so v določeni meri vseeno pozabili na pomembno vlogo neprestanega usposabljanja zaposlenih. Zaposlenih niso pripravili na spremembe v zadostni meri. Vsak zaposleni se seznani z varnostno politiko le takrat, ko se zaposli, ko podpiše izjavo o tem, da jez varnostno politiko dejansko seznanjen in da se z njo tudi strinja. Iz lastnih izkušenj vem, da posameznika prvi dan na delovnem mestu zasujejo z različno dokumentacijo. Tak način seznanitve z varnostno politiko nima posebnega učinka, saj v navalu novih informacij posameznik hitro spregleda pomen le-te. Neučinkovitost tega pristopa se pokaže v praksi, saj prihaja dnevno do varnostnih incidentov. Vse to bi se lahko rešilo s pomočjo enournega izobraževanja po skupinah. Zaposlenim bi morali pokazati, da je varnost podatkov pomembna tudi zanje, saj nosijo odgovornost za kršitve varnostne politike.

Na ostalih področjih pa je ARSKTRP skladna s smernicami, ki jih postavlja standard BS7799. Ta skladnost je tudi posledica vsakoletne revizije, ki jo zahteva Evropska Unija. Vsa področja, ki ne dosegajo zahtev standardov, dobijo negativno oceno, ki jo je treba seveda popraviti v doglednem času. Prav zaradi teh zahtev revizije in skoraj neomejenih sredstev je ARSKTRP razvila zelo sodoben in učinkovit sistem varovanja informacij. Je ena najbolj razvitih tovrstnih agencij v Evropski Uniji. Strokovnjaki z Agencije Republike Slovenije za kmetijske trge in razvoj podeželja obiskujejo novejše članice EU in jim s svojimi izkušnjami in znanjem pomagajo pri razvoju agencije, kakršna mora biti, da ustreza pogojem, ki jih postavlja EU.

Samo varovanje informacij mora biti prilagojeno vsaki organizaciji posebej. Lahko kupimo že izdelan program varovanja informacij, vendar lahko potem pričakujemo težave. Vsaka organizacija ima namreč take ali drugačne posebnosti. Vseh

procesov, ki se tičejo varovanja informacij, se moramo lotiti sistematično. V nasprotnem primeru pride do napak v delovanju sistema, ki pa lahko ogrozijo poslovanje ali prinesejo ogromno dodatnih stroškov.

LITERATURA

1. Beganovič Merima: Načrtovanje in upravljanje varnosti informacijske tehnologije. Ljubljana : EF, 2004. 87 str.
2. Berčič Boštjan: Skladnost varnostnih politik z zakonodajo. Bilten konference infosec 2003 : Nova Gorica, Inštitut za informacijsko varnost, 2003, str. 7-9.
3. Berčič Boštjan et al.: Ukrepi v primeru informacijskih nesreč. Nova Gorica : Inštitut za informacijsko varnost, 2003. 148 str.
4. Damij Talib, Štemberger Indihar Mojca: Uvod v poslovno informatiko in računalništvo. Ljubljana : EF, 1995. 91 str.
5. Frangež Zdenko: Škodljivci na pohodu. Moj mikro, Ljubljana, 2006, št. 4 ,str. 48-51.
6. Hobbs Michael: Audit and security management. London : KPMG, Information security group, 1997
7. Knez Jože: ISO/IEC 27001 v obstoječih sistemih vodenja. Varnostni forum. Nova Gorica : Palsit, 2005, str. 18-19.
8. Konečnik Tadeja: Novi standard za varnost podatkov. Gospodarski vestnik (Priloga I&T), Ljubljana, 2002, str. 22-23.
9. Krkoč Peter: Praktične izkušnje pri vzpostavitvi sistema varovanja vodenja varovanja informacij. Varnostni forum. Nova Gorica : Palsit, 2006, str. 12
10. Makarovič Boštjan et al.: Internet in pravo. Izbrane teme s komentarjem Zakona o elektronskem poslovanju in elektronskem podpisu. Ljubljana : Pasadena, 2001
11. Olovsson Tomas: A structured approach to computer security. Chalmers university of technology Gothernburg : Department of computer engineering: 1992.
12. Rakovec Sašo: Varovanje informacij skladno s standardom BS7799. Magistrsko delo. Ljubljana : EF, 2005. 92 str.
13. Sabadin Rok: Kriptografija in varnost slovenskih e-trgovin. Diplomsko delo. Ljubljana : EF, 2006. 80 str.
14. Zupan Lucija: Stičišča informacijske varnosti in revizije informacijskih sistemov. Varnostni forum. Nova Gorica : Palsit, 2006, str. 14-15.

VIRI

1. Agencija Republike Slovenije za kmetijske trge in razvoj podeželja. [URL: http://www.arsktrp.gov.si/], 6.1.2007.
2. Andolšek Irena, Javornik Boža: Pomembnost plana za neprekinjeno poslovanje za organizacije. [URL: www.drustvoinformatika.si/dogodki/arhiv/dsi2001/sekcija_d/andolsek_javornik.doc], 2.4.2007.
3. British Standard BS 7799-2:2002: Sistemi za upravljanje varovanja informacij-specifikacija s smernicami za uporabo. Nova Gorica : Palsit, 2003. 48 str.
4. Horjak Marjeta: Vpliv varne informacijske tehnologije na ekonomsko uspešnost podjetja. [URL: http://www.mfc-l.si/?s=d&p=horjak2&l=si], 22.2.2007

5. Interni viri ARSKTRP.
6. Kee Kok Chiaw: Security policy roadmap – Process for creating security policies. [URL: http://www.sans.org/reading_room/whitepapers/policyissues/494.php], 10.2.2007.
7. Micro Process d.o.o. [URL: http://www.microprocess.si/vp.html], 27.2.2007.
8. Varnostni forum. [URL: http://varnostniforum.com], 17.2.2007.

Priloga 1: Izjava

IZJAVA

Izjavljam, da sem prebral/-a in razumem vsebino Krovne politike varovanja informacij na ARSKTRP – Izjava vodstva, ter se z njo strinjam.

Ime in Priimek:_____ Podpis:_____

Služba/sektor:_____

Datum:_____

Priloga 2: Zahtevek za dostop do računalniškega sistema

ZAHTEVEK IN POOBLASTILO ZA DOSTOP DO RAČUNALNIŠKEGA SISTEMA ARSKTRP

(Ta list izpolni samo tisti, ki prične z delom na AKTRP na novo)

IZPOLNI VLAGATELJ

1. Služba/Sektor/Oddelek: _____

2. Ime in priimek vlagatelja: _____
(IZPOLNI ČITLJIVO Z VELIKIMI TISKANIMI ČRKAMI)

3. Potrebuje osebni računalnik ☐ DA ☐ NE

4. Posebne zahteve:_____
(Utemeljitev)

	Zahtevana programska oprema (ustrezno označi)	**Usposobljenost vlagatelja** (ustrezno označi)
Lotus Notes / elektronska pošta	☐ DA	☐ DA
Internet	☐ DA	☐ DA

5. Datum: _____

Vodja oddelka

_____
ime in priimek, podpis

Vodja sektorja/službe

_____
ime in priimek, podpis

IZPOLNI SIUT

1.Datum prejema zahtevka: _____

2. Namestitev opravljena dne:_____Namestitev opravil_____

3. Geslo(pravice) dodeljeno dne:_____ Geslo(pravice) dodelil: _____
(geslo je potrebno spremeniti vsakih 30 dni)

4 Namestitev ni bila opravljena (je bila opravljena le delno) zaradi naslednjih razlogov:

Priloga 3: Zahtevek za dostop do podatkov

DOVOLJENJE ZA UPORABO NAMENSKE PROGRAMSKE OPREME IN DOSTOP DO PODATKOV

1. Dovoljujem, da se _____
ime in priimek -**IZPOLNI ČITLJIVO Z VELIKIMI TISKANIMI ČRKAMI**

2.zaposlenemu/ni v_____oddelku_____Uporabniško ime_____
naziv sektorja/službe naziv oddelka (user za prijavo na računalnik)

na delovnem mestu _____ ☐ za nedoločen čas ☐ za določen čas
naziv delovnega mesta

☐ **DOSTOP DO MAPE SEKTORJA (ODDELKA)** **Ime računalnika: AKTRP-W2K-_____**
(dostop do mape oddelka na disku J:)

3. omogoči na njegovem računalniku uporaba računalniškega programa (ustrezno izpolnite):

☐ **LOTUS NOTES APLIKACIJE** **(izpolni prilogo C za Lotus Notes aplikacije)**

Aplikacije: **Obvezno izpolni priloge navedene v oklepaju za željene aplikacije**

☐ ČEBELE 2005 **(A/2)**	☐ NRN 2004 -Toča **(G1)**	☐ Obračun NRN2003**(L)**
☐ SUBVENCIJE 2002 **(lB/1)**	☐ Obračun 2002 **(H)**	☐ Obračun NRN2004**(L/1)**
☐SUBVENCIJE 2003 **(B/2)**	☐ Obračun 2003 **(H/1)**	☐ VINOGRADI_06/PRESVIN **(N)**
☐ SUBVENCIJE 2004 **(B/3)**	☐ Obračun 2004 **(H/2)**	☐ EUS2004 **(O)**
☐ SUBVENCIJE 2005 **(B/4)**	☐Obračun 2005 **(H/3)**	☐ EUS 2005 **(O/1)**
☐ SUBVENCIJE 2006 **(B/5)**	☐Obračun 2006 **(H/4)**	☐ Zgodnje upokojevanje **(R)**
☐ SUBVENCIJE 2007 **(B/6)**	☐ NEUGODNE RAZM. 05 **(I/1)**	☐ SAP **(S)**
☐ DF 2001**(D)**	☐ NEUGODNE RAZM. 06 **(I/2)**	☐ CRS **(T)**
☐ ZT **(E)**	☐ INŠPEKTORSKA 2004 **(J)**	☐ CRV **(T/1)**
☐ X- TABELE **(F)**	☐ INŠPEKTORSKA 2005 **(J/1)**	☐ Sledljivost **(U)**
☐ NRN 2003 –Suša **(G)**	☐ INŠPEKTORSKA 2006 **(J/2)**	☐ SQL Dostop do baz podatkov **(V)**
	☐ ODKUP MLEKA(mlečne Kvote) **(K)**	☐ PREMIJSKE PRAVICE 05 **(Z/1)**

☐ DOSTOP DO OSTALIH MAP NA MREŽNEM DISKU: ☐ **branje** ☐ **Pisanje** **Vpiši ime mape:**

_____

☐ DOSTOP DO SKUPNEGA POŠTNEGA PREDALA ZA : ☐ **branje** ☐ **Pisanje** **Vpiši ime p. predala:**

_____

☐ OSTALO:_____

- Opomba: Izpolnjujte samo tiste rubrike in samo tiste liste ki se nanašajo na vaše področje dela! Obvezno izpolnite odgovarjajočo(e) prilogo(e)! Oddajte samo izpolnjene priloge.

4. V Ljubljani, _____ 5. Vlagatelj:_____
ime in priimek, podpis

Franc Kebe

_____
ime in priimek, podpis

vodja sektorja generalni direktor

Priloga 4: Kontrolna lista preverjanja dokumentacije povezane z varnostjo IS

SIUT-Pregled dokumentacije povezane z varnostjo

KONTROLNA LISTA ZA PREGLED VARNOSTNE DOKUMENTACIJE

	Mesec	**Dokumentacija usklajena DA/NE**	**kontroliral vodja ODP/namestnik**	**Podpis**
1	Januar			
2	Februar			
3	Marec			
4	April			
5	Maj			
6	Junij			
7	Julij			
8	Avgust			
9	September			
10	Oktober			
11	November			
12	December			

Priloga 5: Zahtevek za dodelitev certifikata SIGOV-CA

SIGOV-CA
Overitelj na Ministrstvu za javno upravo

Tržaška cesta 21, 1000 Ljubljana, Slovenija
http://www.sigov-ca.gov.si
sigov-ca@gov.si

SIGOV-CA

Zahtevek za pridobitev kvalificiranih digitalnih potrdil za zaposlene državnih organov

Zahtevek za pridobitev posebnega in/ali spletnega kvalificiranega digitalnega potrdila (*v nadaljevanju* potrdila) za zaposlene državnih organov (*v nadaljevanju* institucij) izpolni predstojnik institucije (minister, generalni sekretar, direktor ali načelnik upravne enote) in eden ali več[1] bodočih imetnikov potrdila, za katere želi institucija pridobiti potrdilo za opravljanje dela za institucijo. Izpolnjeni zahtevek predstojnik institucije na varen način posreduje na SIGOV-CA.

*Prosimo, da zahtevek izpolnite s tiskanimi črkami, pri možnostih izbire se ustrezne označijo z X. Potrdilo vsebuje podatke o instituciji in imetniku potrdila: oznako institucije (velja samo za posebno potrdilo), ime in priimek imetnika, serijsko številko potrdila, e-naslov, številko politike, začetek in konec veljavnosti potrdila, naziv izdajatelja, javni ključ in ostale podatke v skladu s Politiko SIGOV-CA za kvalificirana digitalna potrdila za državne organe (*v nadaljevanju *Politika SIGOV-CA), ki je javno objavljena na spletnih straneh SIGOV-CA. Ostali osebni podatki ne bodo uporabljeni v druge nedogovorjene namene.*

Izpolni predstojnik

Podatki o instituciji

Polno ime institucije: _____

Naslov institucije
Naselje: _____
Ulica: _____
Hišna številka: _____
Poštna številka: _____
Pošta: _____

Podatki o kontaktni osebi institucije[2]

Ime: _____ Priimek: _____

Funkcija: _____ Telefon: _____

E-naslov: _____

[1] V primeru zahtevka za izdajo potrdil za več bodočih imetnikov hkrati je potrebno pripraviti in izpolniti ustrezno število rubrike "Izpolni bodoči imetnik potrdila" oz. stran 3 tega obrazca.
[2] Zaposleni institucije, ki dela na področju informatike in lahko nudi podporo pri uporabi potrdil drugim zaposlenim ter ga s svojim podpisom na zahtevku pooblasti predstojnik za komunikacijo z Overiteljem na MJU.

Podatki o predstojniku institucije[3]

Ime: _____ Priimek: _____

Funkcija: _____ E-naslov: _____

Seznam bodočih imetnikov iz zahtevka[4]

Št.	Ime	Priimek
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		
29		
30		

S svojim podpisom jamčim, da sem seznanjen in da se strinjam z določili iz trenutno veljavne Politike SIGOV-CA. Strinjam se, da so v primeru objave nove politike[5], z dnem veljavnosti le-te, vsa potrdila iz tega zahtevka izdana po novi politiki. Za bodoče imetnike, za katere želim, da se jim s tem zahtevkom izda potrdila, s podpisom jamčim za njihovo identiteto v skladu s Politiko SIGOV-CA in ZEPEP[6]. S podpisom tudi jamčim za resničnost podatkov iz tega zahtevka in se obvezujem, da bom sporočil vsako spremembo podatkov, ki bi vplivala na veljavnost potrdil.

[3] Predstojnik institucije, kjer so bodoči imetniki potrdila zaposleni ali za katerega delajo.
[4] Bodoči imetniki, katerim se izda potrdila na podlagi tega zahtevka in čigar podatki so navedeni v rubriki »Izpolni bodoči imetnik potrdila«. V primeru, da je bodočih imetnikov več kot trideset (30), je potrebno pripraviti temu ustrezno število te strani.
[5] V primeru spremembe Politike SIGOV-CA se le-ta javno objavi osem (8) dni preden stopi v veljavo. Z dnem veljavnosti nove politike pa so vsa potrdila izdana po tej politiki.
[6] Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS št. 57/2000, 25/2004 in 98/2004)

Kraj in datum: _____ Žig in podpis predstojnika: _____

Izpolni bodoči imetnik potrdila[7]

Podatki o bodočem imetniku

Ime: _____ Priimek: _____

Davčna številka [8]: _____ EMŠO[9]: _____

E-naslov: _____

Želim pridobiti potrdilo: posebno: ☐ spletno: ☐

Geslo za preklic potrdila[10]: _____

Podatki o potrebni opremi

Opreme ne potrebujem: ☐ Potrebujem čitalec: ☐ Potrebujem kartico: ☐

Obrazložitev (neobvezno): _____

S svojim podpisom jamčim, da sem seznanjen in da se strinjam z določili iz trenutno veljavne Politike SIGOV-CA. Strinjam se, da je v primeru objave nove politike[11], z dnem veljavnosti le-te, potrdilo iz tega zahtevka izdano po novi politiki. S svojim podpisom jamčim za resničnost navedenih podatkov ter pooblaščam SIGOV-CA, da moje osebne podatke iz tega zahtevka obdeluje za namene elektronskega poslovanja v skladu s Politiko SIGOV-CA ter zakonoma ZEPEP[12] in ZVOP[13].

Kraj in datum: _____ Podpis bodočega imetnika: _____

[7] V primeru zahtevka za več bodočih imetnikov hkrati je potrebno pripraviti in izpolniti ustrezno število te strani.
[8] Podatek ni obvezen, vendar je potreben za opravljanje nekaterih storitev na elektronski način v skladu z nameni uporabe potrdila, kot je določeno v Politiki SIGOV-CA.
[9] Podatek ni obvezen, vendar je potreben za opravljanje nekaterih storitev na elektronski način v skladu z nameni uporabe potrdila, kot je določeno v Politiki SIGOV-CA.
[10] Geslo za preklic potrdila je namenjeno preklicu po telefonu v skladu s Politiko SIGOV-CA. Dolgo je lahko do dvajset (20) alfanumeričnih znakov, sprememba gesla pa je možna le ob osebni spremembi gesla pri SIGOV-CA ali z zašifriranim in digitalno podpisanim zahtevkom z veljavnim potrdilom.
[11] V primeru spremembe Politike SIGOV-CA se le-ta javno objavi osem (8) dni preden stopi v veljavo. Z dnem veljavnosti nove politike pa so vsa potrdila izdana po tej politiki.
[12] Zakon Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS št. 57/2000, 25/2004 in 98/2004)
[13] Zakon o varstvu osebnih podatkov (Uradni list RS št. 86/2004)

Izpolni pooblaščena oseba SIGOV-CA

Ime in priimek pooblaščene osebe: _____

Datum: _____ Podpis pooblaščene osebe: _____

Zahtevek za kvalificirano digitalno potrdilo SIGOV-CA je odobren!

Odobril:
Franc Tomažič

generalni direktor

Ministrstvo za javno upravo
Direktorat za e-upravo in upravne procese