Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Uroš Grilc

Zasnova varnostne politike na področju zdravstva

diplomsko delo

visokošolski strokovni študijski program prve stopnje računalništvo in informatika

Mentor: doc. dr. Mojca Ciglarič

Ljubljana 2012

Besedilo je oblikovano z urejevalnikom besedil LaTeX.

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Tržaška 25
1001 Ljubljana, Slovenija
telefon: 01 476 84 11
01 476 83 87
faks: 01 426 46 47
01 476 87 11
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št. naloge: 00350/2012
Datum: 13.09.2012

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **UROŠ GRILC**

Naslov: **ZASNOVA VARNOSTNE POLITIKE NA PODROČJU ZDRAVSTVA**
SECURITY POLICY DEVELOPMENT IN THE MEDICAL SYSTEM

Vrsta naloge: Diplomsko delo visokošolskega strokovnega študija prve stopnje

Tematika naloge:

Preučite področje varovanja informacij in načrtovanja varnostnih politik. Osredotočite se predvsem na sistem upravljanja varovanja informacij v zdravstvu. Preučite s tem povezane standarde, priporočila in zbirke dobrih praks ter jih ovrednotite glede na uporabnost za izbrano organizacijo. Opredelite postopek vzpostavitve sistema varovanja informacij in izvedite postopek načrtovanja varnostne politike. Opredelite tudi naloge skrbnika informacijske varnosti. V zaključku kritično opišite pridobljene izkušnje ob načrtovanju in vpeljavi varnostne politike.

Mentor:
M. Ciglarič
doc. dr. Mojca Ciglarič

Dekan:
prof. dr. Nikolaj Zimic

Fakulteta za računalništvo in informatiko • UNIVERZA V LJUBLJANI • 2

Namesto te strani **vstavite** original izdane teme diplomskega dela s podpisom mentorja in dekana ter žigom fakultete, ki ga diplomant dvigne v študentskem referatu, preden odda izdelek v vezavo! Glej tudi sam konec Poglavja **??** na strani **??**.

Izjava o avtorstvu diplomskega dela

Spodaj podpisani Uroš Grilc, z vpisno številko **63070439**, sem avtor diplomskega dela z naslovom:

Zasnova varnostne politike na področju zdravstva

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal samostojno pod mentorstvom doc. dr. Mojce Ciglarič,
- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela
- soglašam z javno objavo elektronske oblike diplomskega dela v zbirki "Dela FRI".

V Ljubljani, dne 7. oktobra 2012 Podpis avtorja:

Kazalo

Uporabljene kratice in simboli

ARPANET	Advanced Research Projects Agency Network
CIZ	Center za informatiko v zdravstvu
ISMS	Information security management system
MZ	Ministrstvo za zdravje Republike Slovenije
SUVI	Sistem za upravljanje in varovanje informacij

Povzetek

V pričujoči nalogi se bomo spoznali s konceptom varovanja informacij in sistemom za varovanje informacij v poslovnih okoljih, nato pa se bomo lotili dejanske zasnove sistema za varovanje informacij v organizaciji, ki deluje na področju zdravstva in katere specifike tako še dodatno narekuje trenutno veljavna zdravstvena zakonodaja.

V zasnovi sistema varnostne politike bomo najprej poskušali določiti želen obseg in cilje omenjenega poslovnega podsistema, sledi popis informacijskega premoženja organizacije, nato popis zahtev poslovnih procesov, zatem poskus analize stanja na področju varovanja informacij v organizaciji in na koncu še ocenjevanje in obravnavanje prisotnih tveganj.

Iz dobljenih rezultatov bo sledil razvoj varnostne politike, postopkov dela in potrebnih kontrol, na koncu pa si bomo le še ogledali korake, ki razvojno ekipo čakajo pri nadaljnji vpeljavi novonastalega sistema.

Ključne besede: varovanje informacij, suvi, zdravstvo, zNet

Abstract

In the following assignment, we will research the concepts of information security and information security management system in a business environment. Then we will try to develop an actual information security management system for an organization, active in healthcare area, which will be specified by restrictions, introduced by the current state legislation for the healthcare area.

In the developing information security management system, we will first try to define the desired system's scope and its objectives, then we will make an inventory of organization's IT assets, following by the analysis of business processes requirements on the subject. We will then review current information security precautions in the organization, ending with the evaluation and the assessment of the possible risks to the system.

Given results will then be used for developing security policy documentation, work practices and necessary performance controls. In the end, we will also look at the next steps, security policy development group will have to take, while finishing implementation of the new made system.

Keywords: information security, isms, healthcare, zNet

Poglavje 1

Uvod

Vse večja informatizacija poslovanja v današnjem času s seboj prinaša veliko izzivov, med katerimi vsekakor najbolj izstopa varnost samih informacij, zbranih in obdelanih v tovrstnih poslovnih transakcijah. Zagotavljanje celovitosti, zaupnosti in razpoložljivosti le-teh vsekakor ni enostavno, da pa tovrstne postopke nekoliko poenostavimo in pocenimo, pa se zgledujemo po že uveljavljenih mednarodnih standardih in primerih dobrih praks na tem področju, ki nam jih na kratko predstavi tudi pričujoča naloga.

Povod za seznanitev s tem področjem, je bilo moje praktično izobraževanje na Zavodu za zdravstveno varstvo Kranj, kjer so bili ravno v tem času seznanjeni z nujnostjo vpeljave standardiziranega sistema za upravljanje varovanja informacij, v kolikor se želijo vključiti v nastajajoče državno zdravstveno omrežje zNet. Za nosilca projekta so določili kar mene, ki pa me je, kot boste lahko kasneje iz naloge tudi sami razbrali, čakala občutno težja naloga, kot so bile moje prvotne predstave in načrti zanjo. Projekt se je tako prelevil v zgodbo o nekoliko "zakasnjenem" uspehu, mi je pa za razliko od teoretičnih akademskih praks, ponudil realno izkušnjo upravljanja projekta v poslovnem okolju, ter nepredvidljivih dejavnikih, ki se lahko ob tem pojavijo in jih v nadalje vsekakor velja vzeti v obzir.

Cilj projekta in posledično tudi diplomske naloge je torej praktična izkušnja in opažanja ob zasnovi sistema upravljanja varovanja informacij v organiza-

ciji z zdravstveno dejavnostjo. Najprej si bomo pobližje ogledali kako se varovanja informacij sploh lotevamo, nato kakšne rešitve in uspešne prakse na tem področju že obstojijo, ter katero smo izbrali kot najprimernejšo za naš projekt. Sledi kratek postopek in poročilo z opažanji ob zasnovi sistema, na koncu pa si bomo ogledali še preostale naloge, ki čakajo razvojno skupino pri nadaljnji vpeljavi in vzdrževanju sistema, ter kaj je potrebno še postoriti za uspešno certifikacijo s strani Ministrstva za zdravje Republike Slovenije.

Vsebina bo tako sprva nekoliko bolj teoretične narave, kasneje pa jo bomo, sočasno s pospešenim pridobivanjem praktičnih izkušenj ob izvedbi projekta, dopolnili tudi z našimi ocenami in opažanji posameznih korakov razvoja in tako poskušali zajeti celovit vpogled na dejansko stanje varovanja informacij na primeru izbranega poslovnega subjekta.

Poglavje 2

Varovanje informacij in varnostne politike

Najprej na kratko opredelimo informacije, njihovo vrednost in pa zakaj ter kako se sploh lotevamo njihovega varovanja, kot zanimivost pa si oglejmo še kratko zgodovino varovanja informacij.

Informacije vseh vrst podjetjem in ostalim organizacijam v sodobni družbi, predstavljajo vedno večji poslovni kapital in posledično od akterjev komunikacije zahtevajo tudi temu primerno rokovanje z njimi, pri njihovem zajemu, obdelavi in arhiviranju. Zato so se, začenši predvsem v nedavni zgodovini, skladno z naraščanjem njihove vrednosti in obsega, razvili številni postopki in standardi varovanja, ki nam služijo kot zgledi in dobre prakse, ko tovrstno problematiko rešujemo v naši organizaciji, in določamo poslovanju podjetja lastne načine nadzora, kontrole in pravila, s katerimi poskušamo zaščititi naš informacijski sistem, ter podatke, ki jih le ta proizvaja. Za boljše razumevanje tako najprej natančneje opredelimo predmet zaščite, kako so se problematike lotevali skozi zgodovino, kakšni izzivi nas pri tem spremljajo in pa kakšne rešitve, standarde in dobre prakse ponujajo sodobna tehnologija in odkritja na tem področju.

2.1 Opredelitev varovanja informacij

> Informacija je rezultat procesa interpretacije podatkov. Je obratno sorazmerna verjetnosti pojava določenega dogodka oziroma podatka - manjša kot je verjetnost pojava, tem večja je informacija ob določenemu dogodku - podatku. [24]

Je torej sredstvo, ključno za uspešno in učinkovito izvedbo poslovnih procesov večine podjetij v informacijski družbi, in kot tako, jo je potrebno tudi ustrezno zaščititi. Glede na predvidene potrošnike, informacije delimo na zasebne, interne in pa javne. Vladni urad za varovanje tajnih podatkov o informacijski varnosti pravi sledeče:

> Informacijska varnost [INFOSEC] pomeni varstvo podatkov in informacijskih sistemov pred nezakonitim dostopom, uporabo, razkritjem, ločitvijo, spremembo ali uničenjem. [6]

> Obsega določanje in uporabo ukrepov za zaščito tajnih podatkov, ki se obdelujejo, shranjujejo in prenašajo s pomočjo komunikacijskih, informacijskih in drugih elektronskih sistemov pred naključno ali namerno izgubo tajnosti, celovitosti ali razpoložljivosti, ter ukrepov za preprečevanje izgube celovitosti in razpoložljivosti samih sistemov. Vsebuje tako ukrepe varovanja tajnosti v računalniških sistemih, oziroma računalniško varnost - COMPUSEC (varnost strojne opreme, varnost programske opreme in varnost programsko-strojne opreme), kot ukrepe varovanja tajnosti v komunikacijskih sistemih, oziroma komunikacijsko varnost - COMSEC (varnost prenosnih sistemov - TRANSEC, varnost kriptografskih metod in naprav - CRYPTOSEC, varnost pri elektromagnetnem sevanju elektronskih naprav - EMSEC). Med omenjene ukrepe sodi tudi odkrivanje, dokumentiranje in zoperstavljanje vsem oblikam groženj, usmerjenim tako proti tajnim podatkom, kot proti sistemom, ki tajne podatke obravnavajo. [9]

Slika 2.1: Temeljni vidiki varovanja informacij. [10]

Kot smo že omenili, skušamo zaščititi glavne tri karakteristike informacij, ki jim dajejo določeno poslovno vrednost, in sicer so to: zaupnost, neokrnjenost in razpoložljivost (ang. confidentiality, integrity and availability).

> **Zaupnost** pomeni, da posredujemo ali omejujemo dostop do informacij ali informacijskega vira z vidika zaupnosti oz. ohranjanja tajnosti informacij ali informacijskega vira. **Celovitost** ali neoporečnost pomeni, da obstaja možnost za ugotavljanje sprememb v informacijah in obstoj kontrol, ki so potrebne za zaščito celovitosti in neoporečnosti informacij ali informacijskih virov. **Razpoložljivost** pa pomeni, da so informacije ali nek informacijski vir na voljo takrat, kadar jih potrebujemo. [23]

Povezovanje posameznih infrastrukturnih in programskih rešitev ter postopkov za ravnanje z občutljivimi podatki, je brez celovitega načrta, zavoljo velike verjetnosti anomalij, ki se pri tem utegnejo pojaviti, pogosto vzrok pojavu nesprejemljivo velike stopnje ranljivosti samega sistema. Tudi odlične samostojne varnostne rešitve lahko torej vodijo do neučinkovitega varnostnega sistema, v kolikor niso ustrezno povezane. Zato se pri izdelavi sistema

največkrat poslužujemo pristopa izgradnje od vrha navzdol (ang. top-down approach). Najprej torej preučimo celoten poslovni sistem, njegove akterje, infrastrukturo in morebitne že obstoječe varnostne postopke, nato ocenimo tveganja in ranljivosti katerim je sistem lahko izpostavljen, nadalje pa se lotimo izdelave krovne varnostne politike. To kasneje razdelimo še na področne varnostne politike in iz njih izpeljemo še izvedbena navodila za posamezna opravila v okviru sistema. Na koncu pa sledijo še skladnostni praktični ukrepi, torej prilagoditev same infrastrukture in pa osveščanje akterjev.

> **Varnostna politika** podjetja definira vse vidike varovanja podjetja (tako materialne kot tudi nematerialne), sestavni del te politike pa je varnostna politika informacijskega sistema, z upoštevanjem vseh povezav z ostalimi dejavniki, ki vplivajo na varnost informacijskega sistema kot celote. Je torej celovit pogled na varnost informacijskega sistema in zajema vse dejavnike, organizacijska pravila in postopke, ki kakorkoli vplivajo na varno in zanesljivo delovanje informacijskega sistema. [23]

V taki ali drugačni obliki, je torej nujna za vsako podjetje, ki mu zaupnost, neokrnjenost in razpoložljivost uporabljanih informacij prinašajo poslovne koristi in v veliko primerih celo poslovno prednost, kljub temu pa ji podjetja v Sloveniji šele zadnja leta namenjajo nekoliko več pozornosti, saj njena izdelava, vpeljava in vzdrževanje niso ugodni, v njene koristi pa ni vedno enostavno prepričati tudi zaposlenih oz. bodočih uporabnikov, kar pa je tudi eden ključnih dejavnikov za njen uspeh in uspešno integracijo. Namreč v kolikor akterji prenosa informacij in podatkov ne upoštevajo varnostne politike v celoti, bo le-ta zelo verjetno neučinkovita.

Glede na specifike naših poslovnih procesov lahko izbiramo med tremi tipi varnostnih politik, in sicer **odprto**, **restriktivno** in pa **zaprto**. Prva sledi načelu, da je ponudnikom in potrošnikom določenih informacij dovoljeno vse, kar ni izrecno prepovedano, restriktivna z večjo stopnjo prožnosti, prek njej lastnih metod, natančneje določa pravila za ravnanje z informacijami, zaprta varnostna politika, pa sledi načelu, da je prepovedano vse, kar ni izrecno

dovoljeno. Odprto prevzemajo predvsem podjetja, ki operirajo večinoma s podatki javne narave, zaprto podjetja z večjim deležem občutljivih tajnih podatkov, restriktivno pa tista z bolj razslojeno ciljno publiko uporabnikov informacij.

Glede na široko opredelitev področja ki ga obravnava varnostna politika, jo zavoljo lažje obravnave delimo na naslednje elemente varnostne politike informacijskega sistema (kot osrednjega sredstva pri izdelavi, obdelavi, porabi in arhiviranju informacij) [23]:

- seznam in varnostna klasifikacija vseh informacijskih virov,
- analiza varnostnega tveganja vsakega informacijskega vira,
- organiziranost varovanja informacijskega sistema,
- dolžnosti, pristojnosti in odgovornosti za varovanje informacijskega sistema,
- varnostni elementi v povezavi s človeškimi viri (notranji akti, zaposlovanje, osveščanje, izobraževanje, usposabljanje, spremljanje, nadzor, prenehanje zaposlitve...),
- zagotavljanje varovanega okolja (varovana območja, varovanje opreme...),
- upravljanje z informacijskimi sistemi (postopki in odgovornosti, načrtovanje in prevzem sistema, zaščita pred zlonamerno programsko opremo, skrbništvo...),
- upravljanje omrežij,
- upravljanje z nosilci podatkov,
- medomrežno povezovanje,
- uporaba elektronske pošte,
- uporaba storitev omrežja Internet,
- upravljanje z varnostnimi dogodki, incidenti in okvarami,

- dostop do informacijskega sistema (upravljanje dostopa, odgovornosti uporabnika, nadzor nad dostopom, mobilni dostop, oddaljen dostop...),
- razvijanje, naročanje, prevzemanje in vzdrževanje programske in strojne opreme,
- načrtovanje neprekinjenega poslovanja,varnostne zahteve zunanjih izvajalcev storitev,
- usklajenost z zakonodajo in
- drugi elementi, ki so specifični za izbran informacijski sistem.

2.2 Kratka zgodovina varovanja informacij

Varovanje informacij se že vse od obstoja prvih večjih civilizacij ponaša z razmeroma bogato zgodovino, vendar pa je veda v obsegu kot ga poznamo danes, svoj razcvet doživela razmeroma pozno, kmalu po pojavu prvih računalniških omrežij v drugi polovici 20. stoletja. Prvi so se pri svoji komunikaciji, sicer v nekoliko primitivnejših oblikah, varovanja tajnih informacij posluževali različni vladarji in vojaški uradniki (tu je verjetno najbolj znan Cezarjev kriptografski sistem oz. tajnopis), v gospodarskih sferah pa so se pojavljale zgolj različne oblike knjigovodstva in uporabe žigov za dokazovanje pristnosti izmenjanih dokumentov. S pospešenim razvojem komunikacijske tehnologije na prelomu 20. stoletja, se je nato pričelo počasi stopnjevati tudi zanimanje za varovanje informacij in tekom druge svetovne vojne so se kazali že prvi resnejši koraki v tej smeri (zloglasna tajnopisna naprava Enigma, vojaško zastražene pomembnejše informacijske in komunikacijske točke), ki so se nato še stopnjevali tekom hladne vojne. S pojavom prvega (vojaškega) računalniškega omrežja ARPANET (1969) in kasneje sodobnega interneta, se je začela pojavljati tudi povečana zaskrbljenost upravljavcev teh infrastruktur o njihovi varnosti in tako je že v zgodnjih sedemdesetih letih preteklega stoletja Oddelek za obrambo (ang. Department of defense)

ZDA izdal prvo poročilo z naslovom Varnostne kontrole za računalniške sisteme (ang. Security Controls for Computer Systems), znano tudi kot "Rand Report R-609". Poročilo bi lahko označili kot nekakšen zametek sistemov za varovanje informacij, saj kot prvo dotlej preusmeri razmišljanje o računalniški varnosti ne zgolj na varovanje strojne opreme, pač pa tudi na podatke, uporabnike in infrastrukturo. Hiter napredek komunikacijske tehnologije v zadnjih desetletjih nam je nato postregel z razvojem številnih standardov in ostalih pristopov k varovanju informacij, ki pa se vedno bolj osredotočajo tudi na obravnavo varovanja informacij v gospodarskih okoljih in niso več zgolj v domeni različnih vojaških institucij. V dandanašnji informacijski družbi namreč informacije marsikateri gospodarski organizaciji predstavljajo nepogrešljiv in konkurenčni kapital, zato je zagotavljanje njihove varnosti mnogokrat ključnega pomena za obstoj organizacije.

2.3 Izzivi varovanja informacij

Osrednji izziv varovanja informacij nam vsekakor predstavlja uveljavljanje treh glavnih načel - zaupnosti, integritete in razpoložljivosti. Ob izrednem napredku tehnologije v zadnjih letih, tako za namene ščitenja, kot tudi zlorabe informacij, ter dejstvu, da ne obstaja kak splošni nabor varnostnih ukrepov ali popoln nabor tehnologije, ki bi se ga lahko nekdo poslužil pri izdelavi sistema varovanja informacij v določeni organizaciji, postane tovrstni projekt zelo zapleten in zahteva dobro podkovan strokovni kader. Le-ta lahko namreč temeljito preuči specifike poslovnih procesov v obravnavani organizaciji, zajame vse akterje in sredstva, ki so udeležena v tokovih izmenjave informacij, ter skladno z željami, zahtevami in potrebami vodstva in zaposlenih, v končnem dokumentu varnostne politike zajame celovit nabor pravil, omejitev in ukrepov, ki jih nato podpre še z ustreznimi tehnološkimi rešitvami, primernimi za organizacijo. Le temeljit in celovit pristop reševanja problematike, se namreč odraža v uporabni in učinkoviti sistemski rešitvi, ki bo prepričala zaposlene k izvajanju in našim informacijam ohranila zaupnost,

integriteto in razpoložljivost.

Eden večjih problemov, kot smo ravnokar omenili, je torej tudi praktična vpeljava varnostne politike med zaposlene. Ti imajo zelo pogosto že ustaljene in močno zakoreninjene vzorce delovanja in pristope k reševanju delovnih problemov. Implementacija novih postopkov v delovne procese zato zna vzbuditi nemalo negodovanj, tako je še posebej pomembno redno izobraževanje zaposlenih o tematiki in pa njihovo uvajanje v vpeljana programska in strojna orodja.

Vsemu navkljub pa se je potrebno zavedati, da še tako učinkovit sistem za varovanje informacij, ne bo nikoli popoln, zato je vedno potrebno iskati prave kompromise med varnostnimi ukrepi, ki nam zmanjšujejo tveganja v poslovnih procesih in pa stroški, ki jih ti ukrepi prinesejo.

2.4 Standardi in dobre prakse varovanja informacij

Varovanja informacij se torej lotevamo celovito, s podjetju prilagojeno varnostno politiko, ki zavoljo zmanjševanja stroškov in upoštevanja dobrih praks, priporočljivo temelji na katerem od mednarodnih standardov za področje varovanja informacij.

> Standard je zapisan sporazum, ki vsebuje tehnične specifikacije ter druge natančne zahteve, ki naj bodo stalno uporabljene kot pravila oziroma smernice. Definira karakteristike, ki zagotovijo skladnost materialov, proizvodov, procesov in storitev. [16]

Nekateri standardi dovoljujejo dokaj splošen okvir ciljnih organizacij (npr. serija ISO/IEC 27000), medtem ko se drugi specializirajo na točneje opredeljene panoge in področja (COBIT, ITIL).

2.4.1 ISO/IEC 1799

Sicer že nekoliko zastarel standard ISO/IEC 17799/BS 7799 predstavlja dobro prakso za upravljanje z varnostjo informacij. Ponuja nabor možnih ukrepov za nadzor prepoznanih tveganj, ki so se z leti uporabe v različnih podjetjih po svetu pokazali kot primeri dobre prakse. V enajstih poglavjih je opisanih 133 kontrol, ki so namenjene doseganju 39 različnih ciljev. [11]

2.4.2 COBIT

Standard COBIT (angl. Control Objectives for Information and related Technology) je zbirka nadzornih ciljev, ki predstavljajo najboljšo prakso za upravljanje informacijske tehnologije. Je pripomoček, ki omogoča informatikom analizo tveganja, vgradnjo kontrolnega okolja, razvoj in vzdrževanje zakonitih, varnih in kakovostnih informacijskih sistemov. Glavni namen COBIT je pomagati razvijati lastne politike in postopke za zaščito, varnost in kontrolo v informatiki. [14]

2.4.3 ITIL

ITIL (angl. Information Technology Infrastructure Library) predstavlja prakse za upravljanje informacijskih storitev. Jasen cilj ITIL je oblikovati konkretna navodila, kako uspešno in učinkovito upravljati z informacijsko tehnologijo. ITIL omogoča, da se podjetje lahko osredotoči na aktivnosti z dodano vrednostjo. [22]

ITIL omogoča razumevanje poslovnih potreb, razumevanje odvisnosti od informacijskih storitev, stroškovno opravičenost, uvajanje reda v upravljanje, upravljanje sprememb, zadovoljstvo uporabnikov in rast informacijske zrelosti. [15]

2.4.4 Standardi družine ISO/IEC 27000

Standardi serije ISO/IEC 27000 so družina mednarodnih standardov za upravljanje informacijske varnosti (znana tudi pod imenom "ISMS Family of Standards" ali "ISO27k") in vsebujejo priporočila in nasvete za zagotavljanje zaupnosti, celovitosti in razpoložljivosti informacij. Trenutno je v seriji standardov ISO/IEC 27000 izdanih že preko sedem standardov, v prihodnosti je predvidenih vsaj še štirinajst.

Edini standard v družini standardov ISO/IEC 27000 po katerem se lahko podjetje certificira je ISO/IEC 27001. Vsi ostali standardi družine podajajo le dobre prakse za vpeljavo standarda v različna okolja in situacije, ter metodologijo za vpeljavo. [17]

Standarde ISO objavlja mednarodna organizacija za standardizacijo (angl. Intenational Organization for Standardization) v sodelovanju z mednarodno elektrotehniško komisijo (angl. International Electrotehnical Commission).

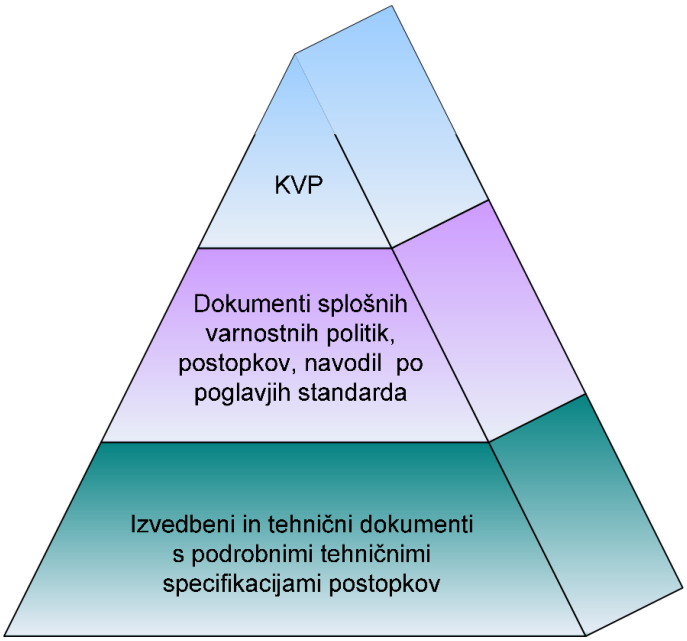
Poglavje 3

Sistem za upravljanje varovanja informacij (SUVI)

Opremljeni s splošnim znanjem varovanja informacij, se sedaj lotimo izbranega sistema za upravljanje varovanja informacij, ki ga bomo kasneje tudi zasnovali za uporabo v izbrani organizaciji. Zato si najprej poglejmo njegovo opredelitev, kakšne omejitve nam pri tem predstavlja obstoječa zakonodaja in pa kje so razlogi za njegovo izbiro.

3.1 Zasnova SUVI

Sistem upravljanja varovanja informacij obsega ljudi, procese in tehnologije. Gre za skupino dokumentov, v katerih so opisani postopki v procesu varovanja informacij in varnostna pravila, ki so odvisna od poslovnih ciljev podjetja, zavezujoča pa so za vse zaposlene v organizaciji. Osredotoča se na varovanje informacij v elektronski in fizični obliki, upošteva tako naravne (npr. požari, potresi, poplave), kot ostale grožnje (npr. industrijsko vohunstvo, zlonamerna koda, vdori v informacijske sisteme, nezaželena elektronska pošta) informacijskemu sistemu izbrane organizacije.



Slika 3.1: Nivoji SUVI. [18, p. 15]

3.2 Splošno o SUVI

Zdravstvenim ustanovam prilagojen SUVI, ki ga je pripravilo Ministrstvo za zdravje Republike Slovenije in na katerega zasnovo se nanaša tudi diplomska naloga, je sestavljen iz treh nivojev, ki jih bomo podrobno opisali v nadaljevanju:

- krovna varnostna politika
- dokumenti splošnih varnostnih politik, postopkov, navodil po poglavjih standarda
- izvedbeni in tehnični dokumenti s podrobnimi tehničnimi specifikacijami postopkov

Z razdelitvijo varnostne politike na več nivojev, dosežemo boljšo preglednost dokumentacije, ter zagotovimo enostaven prehod od strateških ciljev

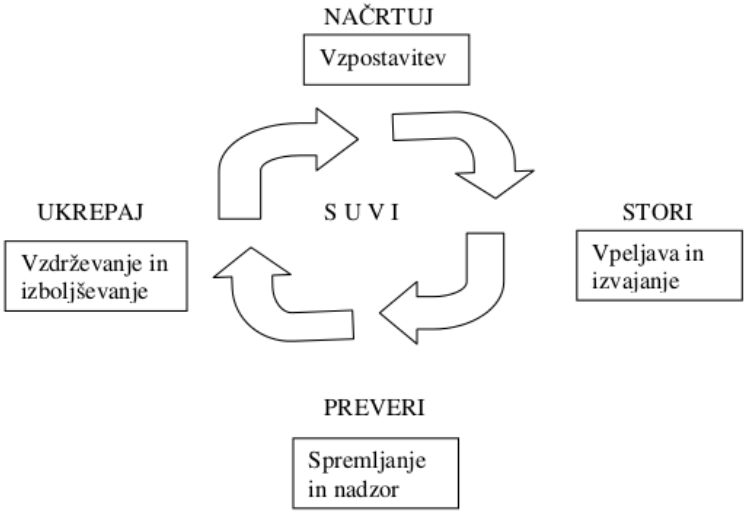
prek mehanizmov do kompletnih postopkov, ki se bodo uporabili za dosego zastavljenih ciljev. [21]

Krovna varnostna politika predstavlja temeljni dokument za varovanje informacij v organizaciji, osnova za oblikovanje celovitega sistema varovanja informacij, iz katerega nato izhajajo podrobnejše področne politike. Krovna varnostna politika vsebuje [21]:

- vloge in odgovornosti,
- temeljna načela delovanja,
- organizacijo dokumentacije,
- usklajenost,
- notranji in zunanji nadzor,
- pregled varnostnih politik za posamezna področja,
- postopek prijave varnostnih incidentov,
- sankcije kršitev,
- veljavnost varnostne politike.

Dokumenti splošnih varnostnih politik, postopkov, navodil po poglavjih standarda nato opredeljujejo postopke in pravila za varovanje informacij v posameznih poslovnih procesih, te pa nato natančneje opredelimo v **izvedbenih in tehničnih dokumentih**, s podrobnimi tehničnimi specifikacijami postopkov, specifičnimi navodili in internimi standardi organizacije, ter postopki za delo (dostop do strežnikov, postopek izdelave varnostnih kopij ipd.).

Za vzpostavitev in upravljanje SUVI uporablja procesni pristop, Demingov model oz. krog odličnosti - načrtuj (plan), stori (do), preveri (check) in ukrepaj (act), kot je prikazano tudi na Sliki 3.2, kar nam torej razkrije tudi



Slika 3.2: Demingov model odličnosti za SUVI. [12, p. 8]

sicer očitno dejstvo, da sistem ni statičen, ampak ga je treba vseskozi prilagajati delovanju organizacije, ga optimizirati in odpravljati napake, lahko bi torej zaključili, da raste in se razvija skupaj z organizacijo.

Faza "načrtuj" mora biti zasnovana tako, da zagotavlja pravilno določitev namena ter okoliščin SUVI. Pomembno je, da so ocene varnostnih tveganj, ki ogrožajo informacije in pripravo načrta za primerno obravnavo teh tveganj, čim bolj pravilne. Podjetje mora tudi vse stopnje faze načrtuj dokumentirati, saj so ti dokumenti pozneje podlaga za upravljanje z morebitnimi spremembami. [21] V fazi "stori" nato vpeljemo izbrane kontrole, ter izvedemo načrtovane aktivnosti, ki smo jih predvideli tekom načrtovanja. Faza preveri od akterja vpeljave SUVI zahteva zagotovitev uspešnega delovanja kontrol SUVI, po potrebi (v kolikor tako zahtevajo spremembe ocen tveganj) SUVI tudi preoblikujemo, zbiramo pa tudi podatke, ki se uporabijo za merjenje uspešnosti SUVI pri doseganju poslovnih ciljev organizacije. Faza "ukrepaj" pa nam nato služi za izvedbo prilagoditev, sprememb in popravkov SUVI ugotovljenih v fazi "preveri", seveda pa moramo o tovrstnih spremembah vseskozi obveščati tudi zaposlene. Omenjene korake nato lahko oprede-

limo še podrobneje, kar bomo storili v nadaljevanju, v poglavju o praktičnih izkušnjah zasnove SUVI v izbrani organizaciji.

3.3 Zakonodaja za varovanje informacij v zdravstvu

Evropska unija je kazensko-pravni okvir zaščite in varnosti informacijskih sistemov uredila v Konvenciji o kibernetskem kriminalu ("Convention on cybercrime") [1], ki obravnava računalniške sisteme in posledice delovanja groženj na organizacije. Ratificirala ga je seveda tudi Slovenija in ga vpeljala med člene svoje ustave in kazenski zakonik. Sicer pa se pri problematiki zdravstvenim ustanovam prilagojenega SUVI, osredotočamo predvsem na zakonodajne člene, ki obravnavajo varnost in zaupnost osebnih in ostalih podatkov, ter člene lastne zdravstveni stroki, ki urejajo delovanje le te, pri rokovanju z občutljivimi podatki. Osredotočamo se torej predvsem na naslednje zakone [18]:

- Zakon o varstvu osebnih podatkov (`http://zakonodaja.gov.si/rpsi/r06/predpis_ZAKO3906.html`)
- Zakon o tajnih podatkih (`http://zakonodaja.gov.si/rpsi/r03/predpis_ZAKO2133.html`)
- Zakon o varstvu dokumentarnega gradiva in arhivih (`http://zakonodaja.gov.si/rpsi/r04/predpis_ZAKO4284.html`)
- Zakon o elektronskih komunikacijah (`http://zakonodaja.gov.si/rpsi/r01/predpis_ZAKO3781.html`)
- Zakon o zdravstveni dejavnosti (47., 51. člen - `http://zakonodaja.gov.si/rpsi/r04/predpis_ZAKO214.html`)
- Zakon o pacientovih pravicah (5., 41., 44., 45., 46. člen - `http://zakonodaja.gov.si/rpsi/r01/predpis_ZAKO4281.html`)

- Zakon o zdravniški službi (50., 51. člen - `http://zakonodaja.gov.si/rpsi/r05/predpis_ZAKO1395.html`)
- Zakon o zbirkah podatkov s področja zdravstvenega varstva (`http://zakonodaja.gov.si/rpsi/r09/predpis_ZAKO1419.html`)

Ti nam morajo torej služiti kot orientacija, pri implementaciji nam lastne SUVI rešitve v naši organizaciji, kot smo že omenili, pa se zakonodaja utegne občasno spreminjati, zato se ji mora sočasno prilagajati tudi naš SUVI.

3.4 Motivacija za vpeljavo SUVI

Primarna motivacija za vpeljavo SUVI v zdravstvenih organizacijah je zagotovo tovrstna zahteva ministrstva za zdravje, kot pogoj k pristopu v nastajajoče zdravstveno omrežje zNet (naslednik omrežja HKOM). Ne glede na to, pa SUVI s seboj prinaša tudi veliko koristi in prednosti izbrani organizaciji, pri njenem poslovnem udejstvovanju. Tu vsekakor prednjači zmanjšanje vpliva na poslovanje zaradi kršitev informacijske varnosti (npr. izguba posla, izguba blagovne znamke, zmanjšanje produktivnosti, povečanje stroškov dela za odpravljanje napak v poslovanju in obnovitev poslovanja, zvišanje zavarovalnih premij in globe), zagotavljanje neprekinjenega poslovanja, zmanjšanje poslovne škode, povečanje donosnosti naložb in poslovnih priložnosti, ohranjanje konkurenčne prednosti, zagotavljanje denarnega toka in zagotavljanje skladnosti z zakonodajo. [13]

Tu so potem še koristi standardizacije postopkov pri preverjanju stanja varnosti informacijskih sistemov organizacije, standardizacija postopkov za komunikacijo z zunanjimi partnerji, dokaz o ustreznosti zaščite informacij za naše poslovne partnerje in splošno standardizirani postopki za boj proti naraščajočim grožnjam varnosti in razpoložljivosti našega informacijskega sistema. Posledično torej vse to pomeni večjo varnost, produktivnost in kredibilnost organizacije. Z vključitvijo v omrežje zNet, pa bo naša organizacija prihranila tudi pri marsikaterem tehničnem mehanizmu zagotavljanja

varnosti (šifriranje podatkov v omrežju, požarni pregradi, identifikaciji in avtorizaciji pacientov, sistem za odkrivanje vdorov in njihovo preprečevanje, ipd.).

3.5 SUVI v zdravstvu

S pričetkom uvedbe projekta eZdravje, septembra 2008 (predviden zaključek junija 2015), so vse zdravstvene ustanove, ki želijo biti povezane v zdravstveno omrežje zNet, pod okriljem Ministrstva za zdravje Republike Slovenije, postavljene pred nalogo vpeljave celovite varnostne politike standardiziranega varovanja poslovnih informacij. Omenjeno ministrstvo je zato v sodelovanju s podizvajalci pripravilo vzorčni predlog varnostne politike oziroma SUVI - sistema upravljanja varovanja informacij, prilagojenega za zdravstvene ustanove in skladnega z zahtevami ministrstva, poleg pa je pripravilo tudi predlog projekta vpeljave SUVI v poslovne procese posameznih institucij. Slednje sedaj čaka še prilagoditev prejetih vzorčnih dokumentov njihovimi poslovnimi procesi in vpeljava nastalega SUVI v poslovanje organizacije, nato sledi notranja presoja ustreznosti izdelanega sistema in na koncu še certifikacija s strani ministrstva, da si s tem pridobijo pravico priklopa v že omenjeno omrežje zNet (Slika 4.1).

Poglavje 4

Projekt zasnove SUVI v izbrani organizaciji

Začeli bomo s kratko opredelitvijo ciljne organizacije, si nato ogledali varnostne zahteve in cilje za nastajajoči sistem, sledil bo kratek opis načrta vpeljave sistema, priloženega s strani koordinatorjev MZ, na koncu pa sledijo še opisi posameznih korakov za pridobivanje potrebnih informacij o poslovnih procesih in pa opisi nadaljnjih korakov, ki čakajo razvojno ekipo, po končani zasnovi sistema za upravljanje varovanja informacij.

4.1 Opredelitev izbrane organizacije

Zavod za zdravstveno varstvo Kranj je neprofitni poslovni subjekt v javni lasti, ki se kljub specifiki lastništva prihodkovno opira predvsem na trg (85%), nekoliko pa torej tudi na državni proračun (15%), trenutno šteje prek 100 dobro izobraženih in kvalificiranih zaposlenih, strankam nudi obsežen sklop storitev, kar pa nam bo kasneje razkrila tudi številčna opredelitev poslovnih procesov. Glede na svojo vpetost v zdravstvene aktivnosti v svoji regiji in izvrševanje strateškega nacionalnega programa zdravstvene preventive, je posledično torej vodilnim vsekakor v interesu, da se zavod vključi v nastajajoče zdravstveno omrežje zNet, za kar pa mora svoje poslovne procese uskladiti

s predpisanimi standardi, med drugim tudi zahtevano, zdravstvenim ustanovam prilagojeno varnostno politiko. V okviru skupnih služb na zavodu deluje tudi služba za informatiko, v okviru katere delujem tudi sam, in ki bo tudi glavni akter pri vpeljavi potrebnih tehnologij za z zahtevami skladno varovanje podatkov in informacij.

4.2 Varnostne zahteve in končno stanje

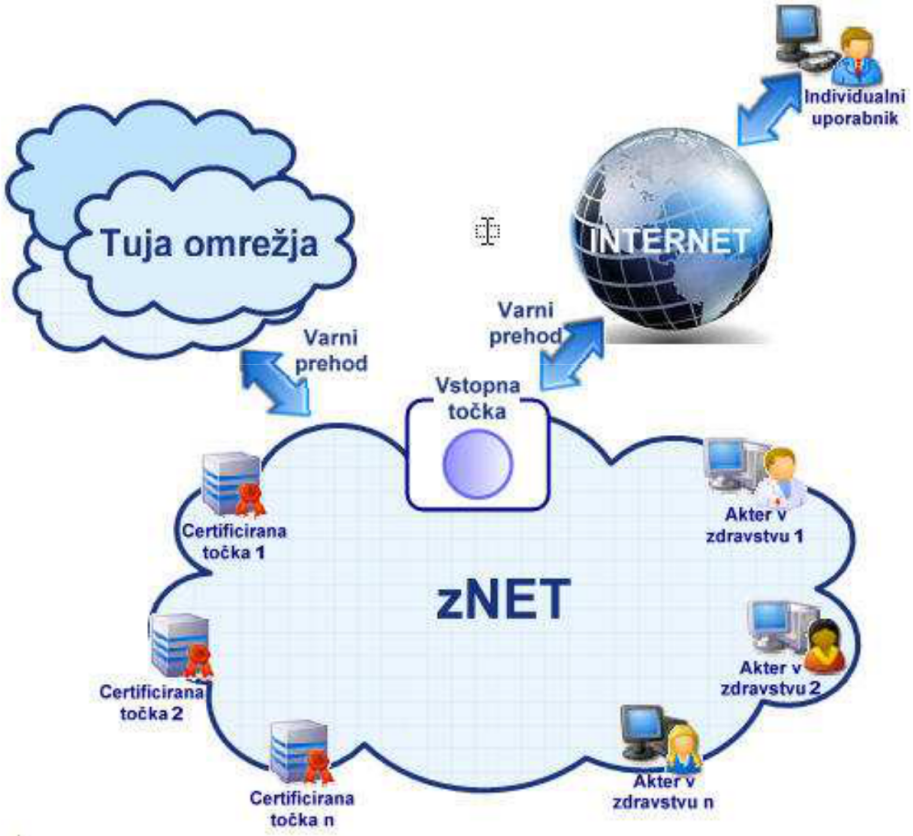
Varnostne zahteve nam v prvi meri predpisuje že zakonodaja. Poleg že omenjenih splošnih zakonov (poglavje Zakonodaja), moramo pri zdravstvenih dejavnostih upoštevati tudi namenske zakone, kot je npr. Zakon o zdravstveni dejavnosti (47. člen, 51. člen), ki vsem udeležencem daje pravico do vpogleda na zdravstveno dokumentacijo, ki se nanaša na njegovo zdravstveno stanje in pa pravico zahtevati, da zdravstveni delavci in njihovi sodelavci brez njegove izrecne privolitve nikomur ne posredujejo podatkov o njegovem zdravstvenem stanju. Tu je nato še Zakon o pacientovih pravicah (5., 41., 44., 45., 46. člen), ki le-te med drugimi definira tudi kot pravico do seznanitve z zdravstveno dokumentacijo in pa pravico do varstva zasebnosti in varstva osebnih podatkov. Zakon o zbirkah podatkov s področja zdravstvenega varstva nato določa zbirke podatkov s področja zdravstvenega varstva, zbiranje, obdelavo in posredovanje podatkov, ki jih pri opravljanju z zakonom določenih nalog vodijo, uporabljajo in medsebojno izmenjujejo pravne in fizične osebe, ki opravljajo zdravstveno dejavnost. Nato je tu še Zakon o zdravniški službi (50. člen, 51. člen), ki zdravnikom določa vodenje dokumentacije o zdravstvenem stanju bolnika in druge evidence v skladu s posebnim zakonom in pa varovanje podatkov o zdravstvenem stanju bolnika in podatkov o vzrokih, okoliščinah in posledicah tega stanja kot poklicne skrivnosti. Zakon o varstvu osebnih podatkov dovoljuje obdelavo osebnih podatkov le, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih osebnih podatkov podana osebna privolitev posameznika, ter določa posebno označevanje in zavarovanje občutljivih osebnih podatkov,

da se tako nepooblaščenim osebam onemogoči dostop do njih. Določa tudi postopke in ukrepe za varovanje osebnih podatkov, ki morajo biti ustrezni glede na tveganje, ki ga predstavlja obdelava in narava določenih osebnih podatkov, ki se obdelujejo, ter dolžnost upravljavcev po zagotavljanju ustreznega zavarovanja osebnih podatkov. Zavarovanje osebnih podatkov v tem kontekstu vključuje organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščeno uničevanje podatkov, njihovo spremembo ali izgubo, ter nepooblaščeno obdelavo, tako da se [18]:

- varuje prostore
- varuje programsko opremo
- preprečuje nepooblaščen dostop
- zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov
- omogoča revizijske sledi pri njihovem rokovanju ali obdelavi

Naloga torej vsekakor ni enostavna, nam pa precejšnji del obveznosti prevzame že skrbnik zdravstvenega omrežja zNet, torej služba CIZ pod okriljem Ministrstva za zdravje Republike Slovenije, ki bo sama poskrbela za varne prehode omrežja z zunanjimi omrežji, spletom in individualnimi uporabniki omrežja zNet, ter njegovo zaščito. Z ozirom na to, da bo naše elektronsko poslovanje potekalo v celoti prek omrežja zNet, nas torej čaka uveljavljanje zahtev varnostne politike na nivoju notranjih procesov organizacije in neposrednih stikov z javnostjo in strankami, ter podizvajalci, in pa nadzor ter preprečevanje morebitnih varnostnih pomanjkljivosti pri prenosih informacij v organizaciji, do vstopne točke zNet (zaščitene morebitne WLAN točke, onemogočeno vohunjenje na komunikacijskih kanalih v okviru organizacije, dostop nepooblaščenih oseb do občutljivih informacij v organizaciji ipd.)

Z uveljavitvijo varnostne politike torej želimo organizacijo uvesti v stanje, kjer bo morebitno tveganje za zlorabo občutljivih informacij kar najmanjše,



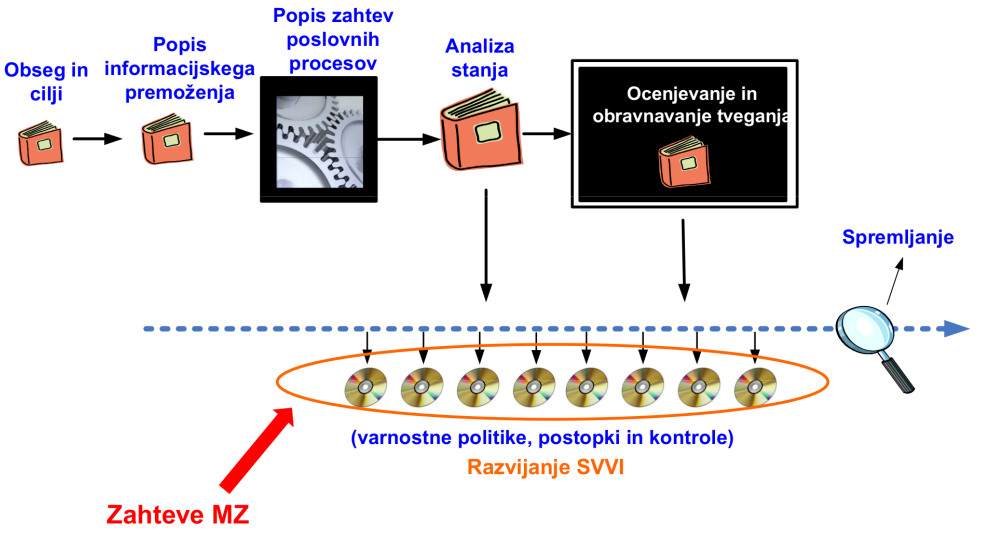
Slika 4.1: Omrežje zNet. [18, p. 10]

zakonsko še dovoljeno - kot vsi vemo, je 100% varnost podatkov realno nedosegljiva, zato si pač razumno določimo še sprejemljive meje, da pri zagotavljanju varnosti podatkov ne paraliziramo vitalnih poslovnih procesov organizacije. To seveda vključuje tako infrastrukturo, kot tudi človeške in ostale vire.

4.3 Načrt zasnove sistema za upravljanje varovanja informacij

Da bi dosegel najhitrejšo in stroškovno čim bolj ugodno vpeljavo varnostne politike, sem se, kot trenutno edini član razvojne skupine, poslužil predlaganega načrta vpeljave varnostne politike, s strani koordinatorjev Ministrstva za zdravje RS [19]. Tako sem se najprej lotil krovnega dokumenta varnostne politike, katerega osnutek so pripravili že koordinatorji z ministrstva, nadaljeval pa s popisom informacijskih sredstev, ki so udeležena pri rokovanju z morebitnimi občutljivimi informacijami. Nato je sledil popis poslovnih procesov in določitev zahtev glede varovanja informacij, zatem še analiza obstoječega stanja, in pa analiza tveganja, ter izdelava varnostnega načrta ukrepov za zmanjšanje nesprejemljivih tveganj. Na koncu je sledila le še priprava dokumentov, postopkov in kontrol varnostne politike, tako da razvojno ekipo čaka le še njena vpeljava v poslovne procese, ko pa bo postorjeno tudi to, pa organizacijo čaka še izvedba notranje presoje in vodstveni pregled ustreznosti novonastalega sistema za varovanje informacij, ob pričetku zastavljenim zahtevam. Po urejenih morebitnih korektivnih ukrepih presojevalcev, sledi še certifikacija sistema, potrebna za vključitev organizacije v omrežje zNet.

Glede na obseg organizacije, interese vodstva in v izogib nepotrebnemu presežku koordinacijskih naporov, posebne projektne skupine za vpeljavo varnostne politike torej nismo oblikovali. Tako sem večino časa deloval na projektu kar sam, skladno s potrebami, pa sem po pooblastilih vodstva lahko za delo na posameznih problematikah aktiviral odgovorne na posameznih področjih. Kar je sicer sprva kazalo na najugodnejšo rešitev izvedbe projekta



Slika 4.2: Postopek vpeljave SUVI. [18, p. 14]

in s kar najmanj posegi v preostale obveznosti zaposlenih pri običajnih zadolžitvah, pa se je na koncu, s padanjem prioritete projekta kot posledice neugodnih gospodarskih dejavnikov in okoliščin, izkazalo kot manj učinkovita organizacijska izvedba.

4.4 Izdelava krovnega dokumenta varnostne politike

Najprej sem se torej lotil krovnega dokumenta varnostne politike, ki določa cilje in osnovne točke informacijske varnostne politike, ter potrjuje pripravljenost vodstva organizacije na postopek vpeljave in nadaljnjo skladnost poslovnega delovanja z varnostno politiko.

V dokumentu je jasno naveden pomen varovanja informacij za izvajalca zdravstvene dejavnosti, opredeljuje nosilca varnostne politike, ki se navadno izbere iz najvišjega vodstva organizacije, zahteva seznanjenost in ravnanje

zaposlenih skladno z varnostno politiko in določa postopke za pregledovanje in spreminjanje varnostne politike. Na kratko pa opredeli tudi osnovna načela varovanja informacij za vsa področja. [19]

Kot že omenjeno, sem tu uporabil kar osnutek dokumenta krovne varnostne politike, ki so ga pripravili koordinatorji iz ministrstva, ter prilagodil nekatere člene, da se skladajo z naravo poslovnih procesov organizacije. Nato pa sem ga kasneje skupaj z dokumenti področnih varnostnih politik, posredoval v potrditev vodstvu, ki je tako izrazilo resnost svojih namer za ta projekt in zavezo k spoštovanju rezultatov le-tega.

4.5 Popis informacijskih sredstev

Sledil je popis informacijskih sredstev, v katerem zajamemo vsa informacijska sredstva v organizaciji, ki so neposredno udeležena pri prenosih, hranjenju, pridobivanju ali manipulaciji informacij.

Popišemo tako [18]:

- informacije v elektronski
- informacije v fizični obliki
- osebje
- strojno opremo
- programsko opremo
- prenosne nosilce podatkov
- komunikacije
- infrastrukturo
- prostore

Za osnovo sem tu uporabil kar zapisnik zadnjega letnega popisa inventarja, ter ob pomoči službe za nabavo, odpravil anomalije, ki so nastale v časovnem zamiku do trenutka našega popisa. Na koncu sem se za potrditev pravilnosti popisa vseeno podal še na hitrejši pregled sredstev po pisarnah, ki bi morebiti ušla popisu inventarja in vseeno lahko prenašala občutljive informacije (cd-ji in dvd-ji, zunanji diski ipd.), izdatno pozornost, pa sem temu področju namenil tudi pri popisu posameznih poslovnih procesov. Za v nadalje, pa sem za ta namen, tekom izvedbe priporočenih ukrepov za skladnost z varnostno politiko, v nabor programskih orodij službe za informatiko, vpeljal tudi programsko rešitev Novell ZenWorks Configuration Management, ki nam v realnem času beleži stanje vseh vključenih delovnih postaj (z nameščeno programsko opremo in priključeno strojno opremo) in ostalih aktivnih informacijskih sredstev.

4.6 Popis poslovnih procesov in določitev zahtev glede varovanja informacij

Nadaljeval sem z opredelitvijo poslovnih procesov in pa zbiranjem podatkov o le-teh, na podlagi katerih sem nato lahko določil potrebno infrastrukturo in ocenil morebitne grožnje ter tveganja.

Ob pomoči poslovnika organizacije, sem njeno delovanje tako razdelil na sledeče poslovne procese:

- Abmulanta
- Dezinfekcija, deratizacija in dezinsekcija
- Epidemiologija nalezljivih bolezni
- Hrup
- Informatika
- Kadrovanje

- Kopalne vode
- Laboratorij za sanitarno kemijo
- Laboratorij za sanitarno mikrobiologijo
- Medicina dela
- Medicinska mikrobiologija
- Nabava
- Nacionalni program
- Odpadne vode in odpadki
- Pitne vode
- Prehrana
- Varstvo pri delu
- Vodenje
- Zrak

Iz seznama teh, nato črpamo orientacijo za zagotavljanje infrastrukture, potrebne za varovanje in upravljanje informacij, nastalih, uporabljanih, urejenih ali arhiviranih tekom naštetih poslovnih procesov. V tem duhu je tako potekal tudi popis poslovnih procesov, in sicer mi je zopet koristila, s strani koordinatorjev MZ predložena predloga za popis poslovnih procesov, kjer sem se osredotočil predvsem na naslednje dejavnike:

- odgovorne osebe poslovnega procesa (lastnik in skrbnik)
- toleriran čas izpada poslovnega procesa
- ocenjena kritičnost poslovnega procesa za dobrobitje ljudi, ugleda organizacije in izpolnjevanje zakonskih zahtev

- informacijska sredstva za podporo poslovnega procesa (informacije, aplikacije in storitve)
- zaupnost informacij, ki so zajete ali proizvedene v poslovnem procesu
- celovitost informacij, ki so zajete ali proizvedene v poslovnem procesu
- ali se lahko proces odvija ob nedelujočem informacijskem sistemu
- v kolikor že obstajajo kaki postopki dela v primeru odpovedi informacijskega sistema
- če zna proces izvajati več oseb, in ni vezan zgolj na eno
- katere osebe so odgovorne za podporo aktivnosti poslovnega procesa
- ali katera od sredstev za aktivnosti poslovnega procesa vzdržujejo zunanji sodelavci
- v kolikor ima akter poslovnega procesa z morebitnimi zunanjimi sodelavci podpisane že kake vzdrževalne pogodbe

V seriji intervjujev oseb, odgovornih za posamezne poslovne procese, sem tako že pridobil jasnejšo sliko stanja na področju varovanja informacij v organizaciji, zbrani podatki pa so predstavljali osnovo za oceno tveganj poslovnih procesov. Ob izdatni pomoči novo pridobljenih informacij sem nato določil še dodatne zahteve za odpravo zaznanih pomanjkljivosti obstoječega sistema za varovanje in upravljanje informacij.

4.7 Analiza stanja varovanja informacij

Sledila je obširnejša analiza obstoječega stanja varovanja informacij, tekom katere sem v iskanju tovrstnih navodil analiziral obstoječo dokumentacijo organizacije, o tem povprašal posamezne vodje poslovnih procesov, na koncu pa na podlagi zbranih podatkov izpolnil vprašalnik, predložen s strani MZ.

6.1.2	Usklajevanje varovanja informacij	Ali se v SUVI vključujejo vsi zaposleni in uporabniki informacijskega sistema organizacije?				Se bodo..
6.1.3	Dodeljevanje odgovornosti za varovanje informacij	Ali so odgovornosti za zaščito posameznih informacijskih sredstev (računalniki, dokumenti itd.) jasno določene?				V praksi, ni še dokumentirano.
6.1.4	Postopek za odobritev zmogljivosti za obdelavo informacij	Ali obstaja postopek, v katerem je potrebna odobritev vodstva za nova informacijska sredstva (strežniška infrastruktura,				Redni letni plan nabave (kolobarjenje).

Slika 4.3: Vzorčni izsek iz obrazca za analizo stanja varovanja informacij.

V njem sem opredelil trenutno stanje organizacije na primeru obširnega seznama varnostnih kontrol, zaključeno delo pa mi je dalo lep seznam potrebnih izvedbenih ukrepov, ki sem jih kasneje upošteval v varnostnem načrtu, razvojna skupina pa bo tudi z njihovo pomočjo tekom vpeljave, poskušala zagotoviti skladnost delovanja vseh poslovnih procesov s standardom ISO/IEC 27001:2005.

4.8 Analiza tveganja in izdelava varnostnega načrta ukrepov za zmanjšanje nesprejemljivih tveganj

Zadosten obseg zbranih informacij, me je privedel do analize tveganja posameznih poslovnih procesov. **Analiza tveganja** je postopek identifikacije groženj in ocenjevanja, kako visoko tveganje te grožnje predstavljajo za orga-

nizacijo. Tveganja ocenimo iz ocene posledic grožnje, verjetnosti uresničitve grožnje, stopnje ranljivosti in učinkovitosti uporabljenih rešitev. **Varnostni načrt** ukrepov za zmanjšanje nesprejemljivih tveganj, pa je seznam ukrepov, s katerimi ocenjena presežna oz. nesprejemljiva tveganja spravimo zopet v meje intervala tolerance, torej sprejemljivih tveganj za organizacijo.

Ponovno se poslužimo predpisane metodologije s strani MZ, kjer prek namenskih tabel, upoštevajočih naštete dejavnike, razberemo oceno stopnje tveganja posameznega procesa.

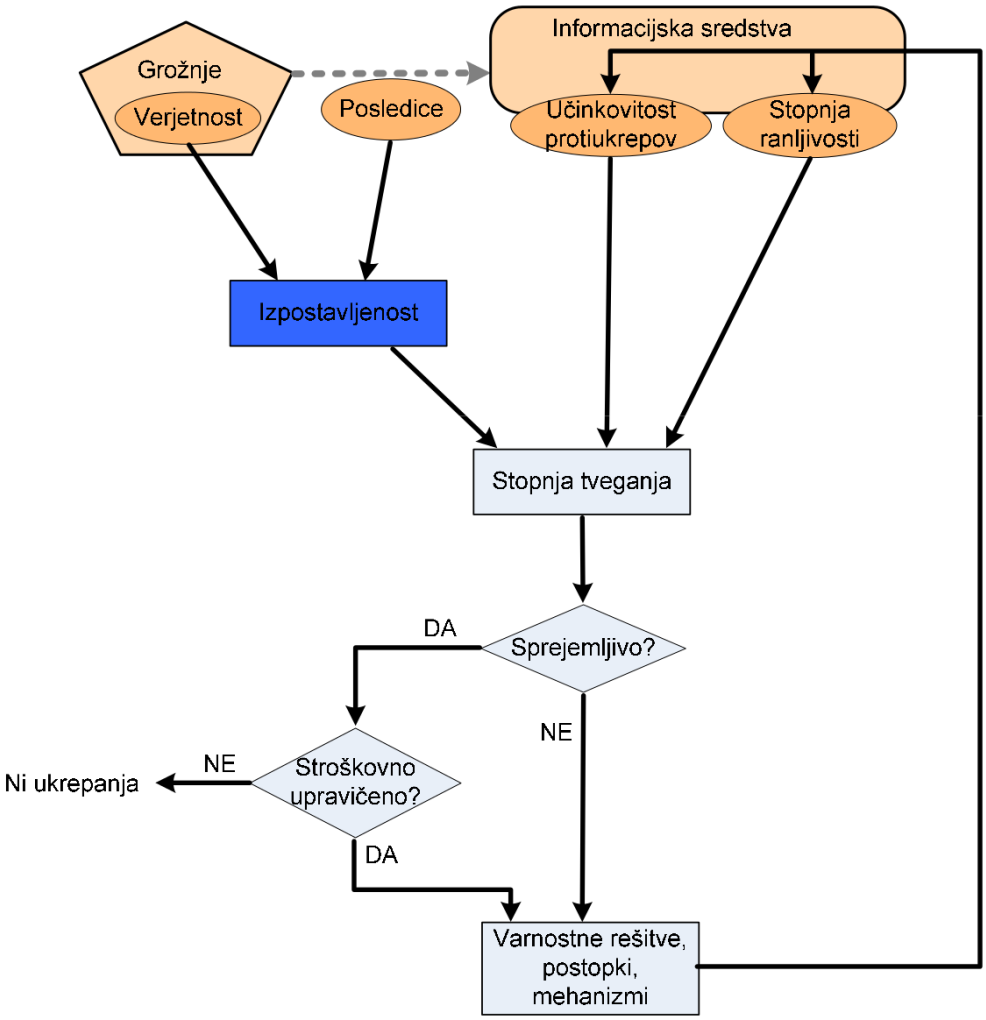
Z ozirom na precejšnjo skladnost varnostnih zahtev vseh poslovnih procesov, sem tu postopek nekoliko poenostavil, in sicer sem za ocene tveganj vseh procesov vzel kar ocenjeno vrednost najbolj kritičnega procesa in jo posplošil na vse ostale. Razen parih izjem, ki so se po varnostnih zahtevah odklanjale tako močno, da sem jih obravnavali individualno - Ambulanta, MD, ENB.

Iz dobljenih rezultatov sem nato izpostavili vse, ki so presegali zastavljeno mejo (vrednosti večje od 3 po predpisani lestvici) in zanje določil korektivne ukrepe, s katerimi bo organizacija uspešno znižala oceno izpostavljenosti do meje sprejemljivega (vrednosti manjše ali enake 3).

4.9 Priprava dokumentov področnih varnostnih politik

Z opravljeno analizo obstoječega stanja varovanja in upravljanja informacij, ter pridobljenimi ocenami izpostavljenosti posameznih poslovnih procesov različnim tveganjem in seznamom korektivnih ukrepov za zmanjšanje le-teh, smo nared za pripravo področnih dokumentov varnostnih politik, s katerimi bomo zagotovili pravno-formalno podlago za izvajanje varnostne politike med predvidenimi akterji.

Tudi tu sem si pomagal kar z vzorci, posredovanimi s strani MZ, področne politike, ki pa so vezane na način organiziranosti, fizično okolje in že vpeljane procese in postopke v naši organizaciji, pa sem skladno preuredil, da ustrezajo našim specifičnim varnostnim zahtevam, lastnostim okolja in procesom.



Slika 4.4: Odločitveni diagram za analizo tveganja. [18, p. 42]

V postopku seveda upoštevamo morebitne korektivne ukrepe, pridobljene v procesu ocene tveganja, ki bi jih morebiti veljalo izrecno poudariti in zapisati.

Področne politike se nato aktivno dopolnjujejo tudi z izvedbenimi postopki in navodili za uveljavljanje posameznih členov politike, ki so sicer v ciljni organizaciji zahtevani že s kontrolami standarda ISO/IEC 27001:2005. Za že zajeta področja sem uporabil kar omenjene dokumente MZ, manjkajoče, pa seveda skladno s potrebami izdelal in dopolnil.

4.10 Predhodna priprava infrastrukture in delovnega okolja

Za nadaljnje postopanje pri izpolnitvi manjkajočih zahtev, sem nato s podrobno preučitvijo nastale dokumentacije varnostne politike izdelal seznam potrebnih opravil, ki sem ga združil s korektivnimi ukrepi iz procesa ocenjevanja tveganj, ter tako dobil seznam nujnih opravil za vzpostavitev primernega okolja in infrastrukture za izpolnjevanje določil varnostne politike, preden spoštovanje le-te zahtevam od zaposlenih, z njihovim podpisom aneksa k pogodbi o zaposlitvi.

Z ozirom na to, da zaposleni večino svojega dela opravijo na računalnikih, ki so tako osrednji pripomočki pri njihovem delu, in da je informacijski sistem organizacije ob precejšnji stagnaciji razvoja v zadnjih letih nekoliko zastarel, sem tu naletel na znatnejšo oviro, katere izvedba je v določenih segmentih še vedno v teku. Po posvetu s strokovnjaki, ki tudi sicer skrbijo za naprednejše posege na našem informacijskem sistemu, sem ob pomoči informatika in podizvajalca pripravil načrt nadgradnje obstoječe opreme z virtualizacijskim strežnikom in podatkovnimi polji, prek katerih smo tako s pomočjo vmWare ESXi in SUSE Linux Enterprise Serverja, obstoječe Novell eDirectory storitve razširili z virtualnimi namenskimi strežniki, kot so ZenWorks Configuration Management, Novell Service Desk in Novell Vibe onPrem.

ZenWorks Configuration Management (`http://www.novell.com/products/zenworks/configurationmanagement/`) bo organizaciji, kot smo

že omenili, služil za oddaljeni nadzor in manipulacijo z delovnimi postajami, prenosniki in ostalo opremo, ter tako poenostavil uveljavljanje varnostnih politik pri uporabnikih, oddaljeno pomoč in spremljanje operativne brezhibnosti strojne in programske opreme.

Novell Service Desk (`http://www.novell.com/products/service-desk/`) organizaciji, kot je razvidno že iz imena, ponuja platformo za enostavno interakcijo z uporabniki v primeru okvar strojne in programske opreme, omogoča pa tudi enostavno javljanje kršitev varnostne politike in pa spremljanje zgodovine servisnih posegov na upravljani strojni in programski opremi.

Novell Vibe onPrem (`http://www.novell.com/products/vibe/`) pa ponuja storitev intraneta in tako omogoča dokumentacijske sisteme, enostavno komunikacijo med uporabniki, revizijo sprememb na dokumentih in podobno.

Že iz predhodne konfiguracije informacijskega sistema pa pri uveljavljanju varnostne politike, poleg specializiranih aplikacij, kot so Infonetovi **MBL** [4], **SBL** [5], **K22** [3], Epi Spektrumov **OrbitaLIMS** [2], in Novellov **Groupwise** [7], opaznejšo vlogo igra tudi **Sophos Endpoint Security and Data protection** [8], ki organizaciji služi tako kot klasična zaščita pred zlonamerno kodo, kot tudi za nadzor uporabnikov, zaščito občutljivih informacij, ter identifikacijo in nadzor nad sumljivimi procesi na delovni postaji.

Vpeljava naštetih novih programskih rešitev, je po predvidevanjih, torej v večini padla name, še preden pa sem dodobra zagrabil za tovrstne delovne naloge, pa so se začele razvijati precej neugodne gospodarske okoliščine, ki so ta proces razvlekle močno prek zadanih projektnih rokov.

In sicer so bili tu prvi aktualni vladni varčevalni ukrepi, ki ustanovam v večinski državni lasti prepovedujejo vsakršno sklepanje razmerij za pogodbeno in študentsko delo brez predhodnega soglasja ministrstva, česar seveda organizacija še vedno ni prejela. Tako se je moj prispevek k delovnim nalogam zavoda v poletnih mesecih drastično zmanjšal (študentsko delo prek podizvajalca v zelo omejenem obsegu in kar nemalo podarjenih brezplačnih delovnih ur), kot da to še ne bi bilo dovolj, pa se je zavod ravno v tem

času namenil izvesti tudi t.i. "kolobarjenje" (menjava z novo) računalniške opreme za izbrane oddelke, kar je ob koriščenju letnega dopusta in ostalih obveznostih glavnega in tudi sicer edinega zaposlenega informatika, zopet vse padlo na moja pleča.

Tako so po navodilih vodstva, z razliko od predhodno zastavljenih načrtov, moji delovniki prioritetno minevali predvsem ob menjavi delovnih postaj in nudenju pomoči uporabnikom pri njihovem uvajanju na prenovljeno delovno okolje, ter gašenju nepredvidenih kritičnih dogodkov na obstoječi delovni opremi informacijskega sistema. Povrh vsega, pa so moje storitve v jesenskem času dodelili še na projekt vpeljave sistema črtnih kod na oddelku za medicinsko mikrobiologijo.

Uvedba varnostne politike je tako zavoljo navidezne ne-nujnosti postala žrtev prenizkih prioritet in razen izdelane zasnove, tako v večini še vedno čaka na praktično vpeljavo v poslovne procese organizacije.

4.11 Izobraževanje in vpeljava varnostne politike med zaposlene

Ko bo pripravljena ustrezna infrastruktura za izvajanje zahtev varnostne politike, čaka razvojno ekipo seznanitev zaposlenih z zahtevami varnostne politike, prek internega izobraževanja (predlagana metoda s strani koordinatorjev ministrstva sicer postavlja izvedbo tovrstnega izobraževanja in podpis zaposlenih k upoštevanju varnostne politike že na sam začetek vpeljave, pred zagotovljeno zadostno infrastrukturo). V tej fazi bo razvojna ekipa tako obstoječe zaposlene seznanila z novostmi, ki jih prinaša vpeljava in zahtevami, katerih izpolnjevanje se od njih pričakuje. Po predhodnem posvetu z vodstvom bo pripravila tudi seznam še neizpolnjenih zahtev varnostne politike, katerih izvedbo se bo delegiralo med skrbnike posameznih poslovnih procesov in zaposlene, odpravila pa bo tudi še morebitne anomalije v samem informacijskem sistemu in sistemu varnostne politike, ter le-tega prilagodila s predlogi zaposlenih. Dokument varnostne politike bodo naložili na vsem

dostopno mesto na interni mreži. Pravice za spremembe krovne in pa področnih varnostnih politik, si bo pridržal skrbnik varnostne politike, pravice za popravke dokumentov tehničnih izvedb, pa skrbniki posameznih poslovnih procesov.

Skrbnik varnostne politike bo po končani vpeljavi le-te obvestil tudi vse zunanje sodelavce, ter posodobil ustrezne člene vzpostavljenih vzdrževalnih in servisnih pogodb, vse udeležence v poslovanju zavoda, poleg zunanjih sodelavcev tudi zaposlene in vodstvo, pa nadalje redno na letni ravni obveščal tudi o morebitnih spremembah dokumentov in postopkov varnostne politike.

4.12 Izvedba notranje presoje in vodstvenega pregleda

Uspešna vpeljava in pridobitev soglasja zaposlenih o spoštovanju varnostne politike, bosta organizacijo ustrezno pripravila na notranjo presojo novonastalega sistema za upravljanje varovanja informacij, ki jo organizacija izvede sama, skladno s kontrolami predpisanimi s strani ministrstva. Cilj tovrstnega postopka je preverjanje učinkovitosti vpeljave in vzdrževanja SUVI v okviru same organizacije. Za lažjo izvedbo postopka se organizacija lahko posluži kar presojevalnega obrazca s kontrolami, podanega iz strani MZ, obravnavana organizacija pa se bo lahko opirala tudi na dolgoletne izkušnje notranjih presoj za vzdrževanje že pridobljenega standarda ISO/IEC 27001:2005. Za presojo se določi in ustrezno izobrazi posebno presojevalno skupino, mehanizem notranje presoje pa se nato doda tudi na koledar obveznih letnih zavodskih aktivnosti.

Podobna naloga po opravljeni notranji presoji in izvedeni oceni tveganja čaka tudi vodstvo, in sicer se bo ravno tako na letni ravni izvajal tudi vodstveni pregled, v sklopu katerega bo vodstvo zavoda ocenjevalo ustreznost SUVI za poslovanje zavoda in pa njegovo učinkovitost pri doseganju zastavljenih ciljev. Cilj vodstvenega pregleda je torej nadzor nad delovanjem SUVI, potrditev in sprejem ocene tveganja, končno poročilo, pa se enako kot

poročilo notranje presoje, nato pošlje tudi na CIZ (Center za informatiko v zdravstvu).

Sicer pa se vodstvo ob potrditvi varnostne politike poleg rednih pregledov zaveže tudi k neprestanemu zagotavljanju potrebnih virov za nemoteno izvajanje dejavnosti varnostne politike, imenuje, kot že omenjeno, skrbnika informacijske varnosti, ter neposredno odgovarja ob incidentih, nastalih ob morebitnem zavestnem neizvajanju in neupoštevanju predloženih ukrepov s strani skrbnika informacijske varnosti.

Po uspešno opravljeni notranji presoji in vodstvenem pregledu, organizacija na ministrstvo poda še namero za certifikacijo, vpeljano politiko pa je nato seveda potrebno tudi ustrezno vzdrževati, kar bomo podrobneje opisali v naslednjem poglavju.

Poglavje 5

Naloge skrbnika informacijske varnosti po vpeljavi SUVI

Kot je bilo nakazano že v predhodnem besedilu, je ena od nalog vodstva organizacije tekom zasnove in vpeljave SUVI tudi, da med svojimi zaposlenimi izbere skrbnika novonastalega sistema, ki bo skrbel za njegovo brezhibno vodenje, vzdrževanje in optimizacijo, ter predstavljal osrednji kanal za komunikacijo s kompetentnimi zunanjimi organi za to področje. Zato vsekakor velja na kratko predstaviti tudi naloge, ki čakajo imenovanega skrbnika informacijske varnosti.

SUVI namreč ni statična tvorba in ga je kot takega potrebno tudi redno preverjati in vzdrževati. Tu je najprej spreminjajoča zakonodaja, skladno s katero posodabljamo tudi zaveze organizacije pri stremenju k optimalni varnosti informacij, naš spreminjajoč informacijski sistem, ki ga moramo vseskozi usklajevati z določili vzpostavljene varnostne politike in pa SUVI sam, ki ga z rednim spremljanjem in pregledovanjem ustreznosti specifikam naših poslovnih procesov, poskušamo vseskozi izboljševati po metodi Načrtuj - Stori - Preveri - Ukrepaj (Demingov model, Slika 3.2).

5.1 Spremljanje zaznanih incidentov

Pooblaščenec informacijske varnosti mora tako v okviru vzdrževanja in izboljševanja vpeljane varnostne politike vseskozi imeti pregled nad pretokom informacij v organizaciji in s strankami, ter javljati morebitne kršitve in ostale varnostne incidente vodstvu organizacije, v primeru resnejših kršitev pa tudi na CIZ. Varnostne incidente se nato s kar najmanjšo poslovno škodo sanira, ter preveri in po potrebi odpravi morebitne anomalije v predhodno izvedeni oceni tveganj. Tovrstno javljanje incidentov pooblaščencu se s členi varnostne politike zahteva tudi od zaposlenih, v naši organizaciji, pa bomo v ta namen koristili že omenjeno programsko rešitev Novel Service Desk, kjer se bo v sklopu javljanja napak in okvar programske in strojne opreme, dodala tudi kategorija javljanja napak, predlogov, incidentov ipd. v zvezi z vpeljanim informacijskim sistemom in njegovo varnostno politiko.

5.2 Izvedba ukrepov

Pooblaščenec informacijske varnosti je zadolžen tudi za nadzor in delno tudi izvajanje ukrepov, opredeljenih po izvedbi ocene tveganja, ki bodo procese in pa informacijsko strukturo organizacije dvignili na raven, skladno s predloženimi zahtevami SUVI. Ukrepe je pooblaščenec dolžan ustrezno evidentirati, določiti odgovorne za izvedbo, spremljati primernost njihove izvedbe in o rezultatih in morebitnih zamudah redno obveščati vodstvo organizacije.

5.3 Spremembe varnostnih politik

Spreminjajoča zakonodaja posledično zahteva tudi ažurno prilagajanje veljavne varnostne politike popravkom in posodobitvam le-te. Pooblaščenca informacijske varnosti zato čaka spremljanje Uradnega Lista RS, ter podobnih glasil o spremembah zakonodaje, morebitne spremembe na področju informacijske varnosti, pa mora nato s pomočjo pravne službe v organizaciji, vključiti v aktualno politiko in od odgovornih zahtevati ustrezne ukrepe,

ki bodo zagotovili ponovno skladnost informacijskega sistema s sprejetimi določili.

5.4 Sodelovanje s CIZ

Večkrat smo omenili tudi že Center za informatiko v zdravstvu (katerega naloge do dejanske ustanovitve prevzema Ministrstvo za zdravje Republike Slovenije), ki bo pooblaščencu predstavljal glavno vez med organizacijo, ki jo zastopa in omrežjem zNet. Ker je CIZ, kot upravitelj omrežja zNet, odgovoren za varnost informacij v sklopu le-tega, je tej službi pooblaščenec informacijske varnosti, kot predstavnik v omenjeno omrežje vključene organizacije, dolžan javljati zaznane incidente, ji pošiljati redna poročila o stanju SUVI v organizaciji, ter jo obveščati o ostalih odkritih nepravilnostih na področju varovanja informacij v organizaciji, oziroma pri uporabi omrežja zNet. Še preden pa se tovrstno razmerje lahko sploh prične, mora v organizaciji na pobudo pooblaščenca CIZ opraviti certifikacijo skladnosti SUVI z njihovimi zahtevami.

Poglavje 6

Certifikacijski postopek

Na koncu sledi le še certifikacijski postopek, s katerim CIZ potrdi SUVI obravnavane organizacije kot skladnega z minimalnimi predpisanimi zahtevami za priklop presojanca v zdravstveno omrežje zNet.

Certifikacija se torej izvede v obliki zunanje presoje organizacije, po njeni vpeljani, z ministrstva za zdravje predlagani politiki primernega varovanja osebnih podatkov, občutljivih osebnih podatkov in pa podatkov samo za interno rabo, poteka pa po sledečem postopku [20]:

- Izvajalec zdravstvene dejavnosti preda celotno dokumentacijo SUVI (popise sredstev, dokumente nižjega nivoja, ki morajo biti skladni z varnostnimi politikami eZdravja) v presojo zunanjim presojevalcem.
  - Izvede se presoja dokumentacije (ali je dokumentacija skladna z varnostnimi politikami in zakonodajo) s strani zunanjih presojevalcev, ki izdelajo pisno poročilo o ugotovitvah presoje.
- Izvajalec zdravstvene dejavnosti prejme poročilo o ugotovitvah presoje in na podlagi priporočil ali neskladnosti sprejme ukrepe, katere mora še zagotoviti do presoje na lokaciji.
  - Po dogovoru z izvajalcem zdravstvene dejavnosti se določi datum presoje na lokaciji.

- Izvajalec zdravstvene dejavnosti se pripravi na presojo in določi osebe, ki bodo sodelovale s presojevalcem pri izvedbi zunanje presoje.
  - Izvede se presoja na lokaciji s strani zunanjih presojevalcev, ki izdelajo pisno poročilo o ugotovitvah presoje in odločijo o certifikaciji končne točke.
- Izvajalec zdravstvene dejavnosti se po presoji brez neskladnosti lahko vključi v eZdravje. V kolikor so podana priporočila jih mora izvajalec zdravstvenih dejavnosti upoštevati in v roku 6 mesecev od presoje podati odgovor o uspešni izvedbi zunanjemu presojevalcu. Izvajalec zdravstvenih dejavnosti je navkljub priporočilom certificiran s strani CIZ (vse njegove naloge v prehodnem obdobju opravlja Ministrstvo za zdravje). V kolikor se ugotovijo neskladnosti na presoji, se mora sprejeti primerne ukrepe, katere mora izvajalec zdravstvene dejavnosti še zagotoviti do določenega datuma, ko se izvede presoja ukrepov s strani zunanjega presojevalca. Če so ukrepi primerno izvedeni, se izvajalec zdravstvene dejavnosti vključi v eZdravje.

Rezultat postopka je torej pridobljen certifikat oz. potrdilo o skladnosti, ki pa ga je treba vzdrževati z rednimi letnimi notranjimi presojami in vodstvenimi pregledi v okviru organizacije, nekoliko manj pogosteje pa se bo izvajalo tudi preverjanje s strani usposobljenih zunanjih presojevalcev, katerih urnik in frekvenco bo organizaciji naknadno posredoval podeljevalec certifikata.

Poglavje 7

Sklepne ugotovitve

Zavoljo zaostrenih gospodarskih okoliščin, je bil moj projekt zasnove SUVI za izbrano organizacijo sicer nekoliko otežen, kljub vsemu pa mi je z izdatnim trudom uspelo izpeljati vse ključne korake izdelave omenjenega sistema, tako določiti obsege in cilje, kot tudi popisati informacijska sredstva in zahteve poslovnih procesov, analizirati obstoječe stanje varovanja podatkov v organizaciji, oceniti in obravnavati tveganja, katerim je izpostavljen informacijski sistem, in pa na koncu izdelati dokumentacijo varnostne politike, določiti praktične postopke za vpeljavo in pa seznam kontrol, za preverjanje njene učinkovitosti. V dobršni meri sem uspel tudi pripraviti potrebno infrastrukturo na področju centralnega informacijskega sistema, tako da razvojno ekipo, ki utegne moje delo nadaljevati, takoj ko bodo to dopuščali razpoložljivi finančni in človeški viri zavoda, čaka še osveščanje zaposlenih o uvedbi in pa vpeljava zahtev v vsakdanjik posameznih poslovnih procesov.

Sicer pa je sistem za upravljanje varovanja informacij podsistem poslovnega sistema, ki ne zagotavlja nujno kratkoročno vidnih pozitivnih vplivov na poslovanje organizacije, zato jo kljub relativni razširjenosti v današnjem času, vodstvo podjetja še vedno sprejema razmeroma zadržano, kot ne-nujni dodatni strošek, ki pa sploh v času aktualne recesije, vsekakor ni dobrodošel. Stališče pa se kaj hitro obrne, ko organizacijo doleti kateri od vse pogostejših incidentov zlorabe občutljivih informacij, ki bi jih uspešno vpeljan in kako-

vosten sistem upravljanja varovanja informacij lahko učinkovito preprečil.

Verjamem da naša organizacija tu vsekakor ne nastopa kot osamljen primer. Pri razvrščanju prioritet, v nameri prilagajanja razmeram na trgu, namreč vodstvo velikokrat na razvojne dejavnosti gleda zelo kratkoročno. Tako se podpirajo predvsem dejavnosti, ki ponujajo hitre obliže zadanim ranam poslovanja organizacije, in ji tako omogočajo kratkoročni obstoj, pozablja pa se na dolgoročni strateški vidik razvoja poslovanja organizacije za naslednja desetletja, kjer pa po mojem mnenju, z ozirom na razmah informacijsko-komunikacijske tehnologije v zadnjih letih, ter posledično tudi s tem povezanih kriminalnih dejavnosti, uspešen sistem upravljanja varovanja informacij vsekakor pomeni občutno konkurenčno prednost, sploh ko govorimo o visoko tehnoloških podjetjih, ki svoje dejavnosti usmerjajo k ustvarjanju visoke dodane vrednosti in jim znanje in informacije predstavljajo nepogrešljiv kapital.

Zato tudi z vidika vodstva naše organizacije, ki je trenutno angažirano predvsem za obstoj zavoda v obstoječi obliki (Ministrstvo za zdravje je namreč nedavno napovedalo združevanje proračunsko financiranih dejavnosti v sklop centralnega Inštituta za varovanje zdravja, ter ukinjanje obstoječih tržnih dejavnosti, ki predstavljajo veliko večino poslovnih procesov zavoda) in ohranjanju pozitivne poslovne bilance, vedenje vodstva popolnoma razumem in ga ne obsojam, vsekakor pa mu toplo priporočam, da vpeljavi SUVI zopet vrnejo večjo podporo, brž ko bo to mogoče. Sicer bo omenjen obstoj le pirova zmaga, ki bo vodila v precej megleno in nekonkurenčno prihodnost.

Literatura

[1] (2012) Convention on Cybercrime. Dostopno na: http://conventions.coe.int/Treaty/en/Treaties/html/185.htm

[2] (2012) EpiSpektrum OrbitaLIMS. Dostopno na: http://www.epi-spektrum.si/?nStran=vsebina&mid=58

[3] (2012) Infonet K22. Dostopno na: http://www.infonet.si/products/k22

[4] (2012) Infonet MBL. Dostopno na: http://www.infonet.si/products/mbl

[5] (2012) Infonet SBL. Dostopno na: http://www.infonet.si/products/sbl

[6] (2012) Informacijska varnost. Dostopno na: http://sl.wikipedia.org/wiki/Informacijska_varnost

[7] (2012) Novell Groupwise. Dostopno na: http://www.novell.com/products/groupwise

[8] (2012) Sophos Endpoint Security and Data protection. Dostopno na: http://www.sophos.com/en-us/products/endpoint/endpoint-protection.aspx

[9] (2012) Urad vlade RS za varovanje tajnih podatkov. Dostopno na: http://www.uvtp.gov.si/si/delovna_podrocja/informacijska_varnost

[10] (2012) Vodenje varovanja informacij. Dostopno na: http://www.palsit.com/slo/storitve.php?page=48

[11] S. Bobek, *Uvajanje sistema vodenja varovanja informacij v družbi*, 2007. Dostopno na: http://epf-oi.uni-mb.si:8000/Management_informatike/07_UVAJANJE%20SISTEMA%20VODENJA%20VAROVANJA%20INFORMACIJ%20V%20DRU%C5%BDBI.pdf

[12] *British Standard BS 7799-2:2002: Slovenski prevod standarda, Information security management systems. Specification with guidance for use. [Part 2]*, Nova Gorica: Palsit, 2003, str. 8.

[13] D'Ardenne Associates Ltd., *ISO 27001:2005 Information Security Management Systems*, ZDA, 2012. Dostopno na: http://www.dardenneassociates.com/iso-27000

[14] Governance Institute, *COBIT 4.1*, Ljubljana: ISACA, 2011.

[15] A. Groznik, *Okviri in standardi kakovosti pri reviziji in vodenju informatike*, 2011, str. 39. Dostopno na: http://miha.ef.uni-lj.si/_dokumenti3plus2/196062/AG_standardi.ppt

[16] D. Košćak, *Varovanje informacij v skladu s standardom ISO 27000*, 2011, str. 19. Dostopno na: http://eprints.fri.uni-lj.si/1362/1/Koscak_D.1.pdf

[17] P. Krkoč, *Standarnizirana vpeljava sistema neprekinjenega poslovanja*, Ljubljana: Fakulteta za varnostne vede, 2009.

[18] M. Ozimek, M. Žele, *Implementacija varnostne politike pri izvajalcih zdravstvene dejavnosti*, gradivo k izobraževanju v OE Kranj, Ljubljana, 2011. Dostopno na: http://www.zdrzz.si/files/Gradivo%20za%20izobrazevanje_varnost_KR.pdf

[19] M. Ozimek, M. Žele, *Implementacija varnostnih politik v zdravstvenih zavodih z lastno službo za informatiko*, vzpostavitveni doku-

ment, Ljubljana, 2010. Dostopno na: `http://www.zdrzz.si/files/VDP1-Implementacija%20varnostnih%20politik_koncna%201.0.pdf`

[20] M. Ozimek, M. Žele, *Postopek certificiranja končnih točk in vzdrževanja certifikata*, interno gradivo, Ljubljana, 2009.

[21] S. Rakovec, *Iskraemeco vzpostavlja celovit sistem obvladovanja informacijske varnosti*, Varnostni forum, feb. 2005, str. 6-7, 33.

[22] R. Sajovic, *Upravljanje IT storitev (ITIL). Evolucija, ki jo je odkril že Darwin!*, Ljubljana: Računalniške novice, marec 2011, str. 32.

[23] M. Štrakl, "Varnostna politika informacijskega sistema", *14. Delavnica o telekomunikacijah Vitel*, Brdo pri Kranju, Slovenija, maj 2003, str. 19-20. Dostopno na: `https://lms.uni-mb.si/vitel/14delavnica/clanki/marjan_strakl.pdf`

[24] T. Vidmar, *Informacijsko – komunikacijski sistem*, Ljubljana: Pasadena, 2002, pogl. 1, 14.