Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Luka Florjančič

Varnostna politika podjetja

diplomsko delo

visokošolski strokovni študijski program prve stopnje računalništvo in informatika

Mentor: prof. dr. Marko Bajec

Ljubljana, 2016

Besedilo je oblikovano z urejevalnikom besedil LaTeX.

Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Tematika naloge:

Zaradi čedalje večje povezanosti in elektronskega poslovanja je zagotavljanje informacijske varnosti v podjetjih velik izziv. Podjetja se z njim spoprijemajo tako, da sprejmejo ustrezno varnostno politiko. V diplomskem delu preučite teorijo zagotavljanja informacijske varnosti, vključno s standardi, ki so na voljo, ter za konkretno organizacijo izdelajte dokument varnostne politike. Dokumentirajte izkušnje, ki jih boste pri tem pridobili.

Izjava o avtorstvu zaključnega dela

Spodaj podpisani Luka Florjančič, vpisna številka 63100054, avtor zaključnega dela z naslovom:

Varnostna politika podjetja (angl. *Company security policy*)

IZJAVLJAM

1. da sem pisno zaključno delo študija izdelal samostojno pod mentorstvom prof. dr. Marka Bajca;
2. da je tiskana oblika pisnega zaključnega dela študija istovetna elektronski obliki pisnega zaključnega dela študija;
3. da sem pridobil/-a vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v pisnem zaključnem delu študija in jih v pisnem zaključnem delu študija jasno označil/-a;
4. da sem pri pripravi pisnega zaključnega dela študija ravnal/-a v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil/-a soglasje etične komisije;
5. soglašam, da se elektronska oblika pisnega zaključnega dela študija uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;
6. da na UL neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve avtorskega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja pisnega zaključnega dela študija na voljo javnosti na svetovnem spletu preko Repozitorija UL;
7. dovoljujem objavo svojih osebnih podatkov, ki so navedeni v pisnem zaključnem delu študija in tej izjavi, skupaj z objavo pisnega zaključnega dela študija.

V Ljubljani, dne 07. marca 2016 Podpis študenta/-ke:

Zahvaljujem se svojemu mentorju prof. dr. Marku Bajcu za strokovno svetovanje in nasvete pri pisanju diplomskega dela. Zahvaljujem se tudi staršem in vsem mojim bližnjim, ki so me podpirali skozi vsa leta študija. Hvala vsem za vse spodbudne besede.

Kazalo

Seznam uporabljenih kratic

kratica	angleško	slovensko
IKT	information and communications technology	informacijsko-komunikacijska tehnologija
ISO	international organization for standardization	mednarodna organizacija za standardizacijo
IEC	international electrotechnical commission	mednarodna komisija za elektrotehniko
BS	British standard	Britanski standard
ISMS	information security management system	sistem vodenja varovanja informacij
UPS	uninterruptible power supply	brezprekinitveno napajanje
USB	universal serial bus	univerzalno serijsko vodilo
VPN	virtual private network	navidezno zasebno omrežje
URL	uniform resource locator	enolični krajevnik vira
CIZ		center za informatiko v zdravstvu
SUVI		sistem za upravljanje varovanja informacij
ZD		zdravstveni dom

Povzetek

Naslov: Varnostna politika podjetja

Informacije so postale zelo pomemben dejavnik in temeljni vir v organizaciji. Za uspešno poslovanje podjetja je pomembno obdelava in varovanje informacij, s katerimi podjetje razpolaga. Pri varovanju informacij je pomembno, da te ohranjajo celovitost, zaupnost in razpoložljivost. Če informacije pridejo v napačne roke, ima lahko to resne posledice za podjetje in njegovo poslovanje. Pomembno je, da se nevarnosti zavedajo tako vodstvo kot zaposleni v podjetju. Varnostna politika tako predstavlja nekakšna pravila in pomoč zato, da bi se izognili incidentom in bi se posledice zmanjšale. Je dokument, na katerem lahko razvijemo učinkovit in celovit program informacijske varnosti v podjetju. V diplomski nalogi sem opisal teoretične osnove s področja informacijske varnosti in določenih standardov, ki so najbolj uveljavljeni za varovanje informacij. Izdelava varnostne politike je kompleksen postopek, ki poteka v več fazah. Tako smo upoštevali vse faze in izdelali varnostno politiko za specifično podjetje.

Ključne besede: varnost informacijskega sistema, standardi varovanja informacij, varnostna politika.

Abstract

Title: A Company's Security Policy

Information has become a significant factor and a primary source in any organization. A successful business depends upon the processing and security of information at its disposal, which must remain integral, confidential and available at all times. If the information falls into the wrong hands, a company and its business activities may be confronted by serious consequences. Both management and employees should be aware of such risks. Security policy thus represents the rules and guidelines on how to avoid incidents, or at least, how to minimize the consequences. It has a form of a document, on which effective and comprehensive programme of company's information security policy is based. This thesis describes the theoretical foundations for information security and its established standards. Developing security policy is a complex process that takes place in several stages. In formulating a security policy for a specific company, we considered all of them.

Keywords: information system security, information security standards, security policy.

Poglavje 1

Uvod

Danes živimo v svetu, ko je varovanje informacij eden izmed najpomembnejših dejavnikov za uspešno delovanje podjetja. V sodobnem digitalnem svetu vse več podjetij uporablja informacijsko tehnologijo, s katero povezujejo in podpirajo svoje poslovne procese. Posledica tega je celotna odvisnost podjetja od delovanja informacijske tehnologije, katere je namen olajšati delo in povečati nadzor nad poslovanjem. Vsako podjetje ima željo po uspešnem in varnem poslovanju. Razvoj informacijskih komunikacijskih tehnologij (IKT) je prinesel velike novosti na področju poslovanja. Posledica razvoja in vse pogostejše uporabe informacijskih tehnologij pa je tudi vse večja potreba po varnosti. Zaradi tega mora biti varnost informacijskega sistema eden izmed primarnih ciljev vsakega podjetja in se je s tem potrebno stalno ukvarjati. Podatki in informacije, ki so na računalnikih in svetovnem spletu in se prenašajo po IKT kanalu, so lahko ključnega pomena za poslovanje, zato jih je potrebno ustrezno zaščititi.

Za učinkovito zaščito in zagotavljanje potrebnih ciljev varovanja informacijskega sistema je potreben organiziran pristop in ozaveščenost zaposlenih. Problemov in nevarnosti, ki ogrožajo podatke in informacije, se morajo zavedati vsi zaposleni v podjetju, predvsem pa vodstvo. Zmanjšanje varnostnega tveganja je pomemben dejavnik programa zagotavljanje varnosti, ki ga vodi vodstvo. To dosežemo s pravili, ki jih zapišemo v poseben dokument, ki

definira vse vidike varovanja podjetja. Pravila je potrebno zaposlenim tudi predstaviti in jih ustrezno izobraziti s področja, na katerem delujejo. Tak dokument, ki vsebuje pravila varovanja podjetja tako na fizični kot informacijski varnosti, imenujemo Varnostna politika podjetja. Varnostna politika predstavlja tako osnovni temelj, na katerem lahko razvijemo učinkovit in celovit program varnosti, zato bi ga moralo imeti vsako podjetje. Dokument pripomore k varnosti podjetja, predvsem s stališča uporabnikov, ki se zavejo groženj in tako lahko preprečijo nevarnost, ki lahko vodi tudi do propada podjetja.

V diplomskem delu bom izdelal varnostno politiko za natanko določeno podjetje. Proces izdelave vsebuje pogovor z vodstvom podjetja in seznanitev s trenutnim stanjem varnosti v podjetju. Seznaniti se je potrebno s primarno dejavnostjo delovanja podjetja, s katero se ukvarja, in poslovanjem podjetja. V prvi fazi bom pregledal in preučil ustrezno literaturo, ki se na naša na varovanje informacij. Preučil bom tudi priznane standarde s področja informacijske varnosti. Nato sledi izdelava varnostne politike in ponoven pogovor z vodstvom. Ob morebitnih željah vodstva se bo seveda varnostna politika ustrezno spremenila in na željo njihovih predlogov ustrezno dopolnila. Varnostno politiko bom izdelal na podlagi organiziranosti podjetja in njihove strukture. V pomoč bodo tudi že napisana pravila in standardi s področja informacijske varnosti, ki predstavljajo dobro prakso le-te.

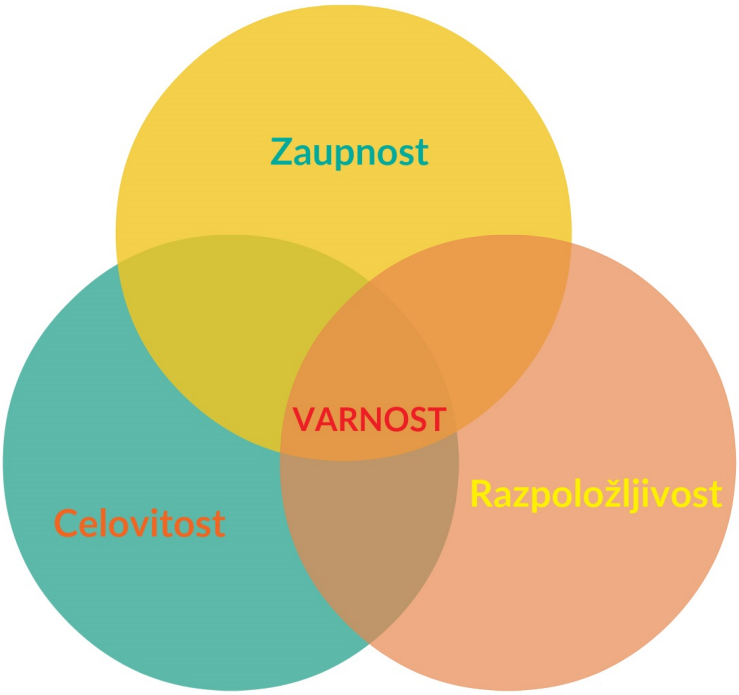
Poglavje 2

Varovanje informacij

Eden izmed glavnih postopkov je varovanje informacij in informacijskega sistema. V današnjem času živimo v družbi, kjer so informacije ključnega pomena. Zato je varovanje le-teh velik izziv, s katerim se morajo spopadati vsi ne glede na področje dela. Informacijski sistemi obdelujejo podatke, od katerih je odvisno naše vsakdanje življenje. Zavedati se moramo, da je vsaka informacija, podatek lahko ključnega pomena, zato jih je potrebno ustrezno zaščitit. Za prenos informacij se v današnjih časih uporabljajo informacijsko komunikacijski kanali. Če IKT ustrezno ne zaščitimo in nepooblaščena oseba razkrije informacije, lahko to privede do katastrofalnih posledic. Varovanje informacijskega sistema je načrt oziroma so postopki zaščite programske in strojne opreme, podatkov, fizičnih naprav, omrežij, zaščita zaposlenih in infrastrukture pred nesrečami, namerno škodo in naravnimi nesrečami. Samo osebje za informacijsko varnost pa ni dovolj. Zelo pomembno je tudi ozaveščanje zaposlenih o vrednosti podatkov, s katerimi delajo, in potrebno jih je seznaniti in izobraziti o ustreznem varovanju, da lahko sami zmanjšajo posledice, ki bi privedle do neželenih dogodkov.

Ko govorimo o varovanju informacij in informacijskega sistema, moramo upoštevati tri cilje – karakteristike, ki predstavljajo ustrezne poslovne procese za uspešno poslovanje podjetja:

- zaupnost,
- celovitost,
- razpoložljivost.



Slika 2.1: Povezava med cilji informacijske varnosti.

Zaupnost informacij pomeni, da posredujemo in omejimo dostop do informacij le avtoriziranim uporabnikom. Do posameznih informacij lahko dostopajo le pooblaščene osebe.
Celovitost pomeni, da informacije ostanejo nespremenjene. Integriteto podatkov lahko spreminjajo in posodabljajo le pooblaščene osebe.

Razpoložljivost informacij pa pomeni, da do informacij in informacijskih virov lahko dostopamo takrat, ko jih potrebujemo. Informacije in njihovi viri morajo biti dostopni ob vsakem času.
Če so vse tri karakteristike informacijskega sistema uspešno dosežene, lahko govorimo o relativno varnem informacijskem sistemu.

Varnost v osnovi pomeni, da se izognemo nevarnostim. Zato je zelo pomembno, da prepoznamo nevarnosti, ki nam pretijo. Absolutno varnega sistem ni. Vsak informacijski sistem je izpostavljen nevarnostim. Visoko stopnjo nevarnosti predstavlja razkritje informacij, ki lahko povzročijo katastrofalne posledice za poslovanje in velike izgube. Druga tveganja, ki še grozijo podjetju, so kraja, nepazljivost zaposlenih in naravne nesreče. Varovanje mora biti usmerjeno in v celovito preprečevanje potencialno možnih nevarnosti. Veliko teh nevarnosti lahko predvidimo in se jim ob primernem ravnanju tudi izognemo. Za večjo varnost v podjetju zato potrebujemo pravila, ki opozarjajo na varnost. Vsem incidentom se ne moremo izogniti; v primeru le-teh nas vodstvo z napotki, ki so zapisani v dokumentu, opozarja in predpisuje, kako ustrezno reagirati ob nastopu incidenta. Taka pravila in navodila o ozaveščanju o nevarnosti in o tem kako naj zaposleni ravnajo, so zapisana in združena v dokumentu Varnostna politika podjetja.

Poglavje 3

Varnostna politika

Osnovni namen varnostne politike je obveščanje uporabnikov, zaposlenih in managerjev o bistvenih zahtevah, ki morajo biti izpolnjene za učinkovito varovanje ljudi, strojne in programske opreme in informacij. [4]

Definicija pojma varnostna politika informacijskega sistema je naslednja: Varnostna politika informacijskega sistema je celovit pogled na varnost informacijskega sistema in zajema vse dejavnike, organizacijska pravila in postopke, ki kakorkoli vplivajo na varno in zanesljivo delovanje celotnega informacijskega sistema. [3]

Varnostna politika je osnova varnostnega načrta v podjetju. Napisana mora biti jasno in enostavno z namenom uporabe za končne uporabnike, da jo bodo razumeli tudi nevešči uporabniki. Napisana je lahko kot en sam dokument, ki zajema vse dele varnostne politike, lahko pa je razdeljena na posamezne enote.

Dokument varnostne politike je v lasti vodstva. Vodstvo je odgovorno za uveljavitev in potrditev dokumenta v podjetju, prav tako je pomembno, da so vsi zaposleni seznanjeni in poučeni o sami varnostni politiki podjetja. Izdelovalec dokumenta tako postane lastnik varnostne politike, ki je ob pobudi vodstva tudi zadolžen za njegovo vzdrževanje in preglede.

Vsako dejanje, ki škoduje podjetju, pa naj gre za namerno ali nenamerno, se obravnava kot kršenje varnostne politike. Zato dobro napisana varnostna

politika vsebuje informacije in pravila o tem, kaj storiti v primeru incidenta, da se tako izognemo hujšim posledicam, ki lahko nastanejo. Vsako podjetje bi moralo imeti varnostno politiko. Varnostna politika se pri posameznih podjetjih razlikuje zaradi specifičnosti poslovanja. V samem dokumentu je vsebovana tudi informacijska varnostna politika. V preteklih letih so informacijsko varnost zanemarjali in so jo omenjali le v nekaterih korakih varnostne politike. Tako je bil pristop le delen. V današnjih časih pa je informacijska varnost zelo pomembna. Tako je prišlo do spoznanja, da je za uspešno poslovanje potrebno informacijsko varnostno politiko vpeljati in uveljaviti. V diplomskem delu sem se osredotočil na varnostno politiko informacijskega sistema, ki je v nadaljevanju poimenovana kot varnostna politika.

Varovanje informacijskega sistema zajema tri karakteristike, ki predstavljajo ustrezne poslovne procese, ki jih od informacijskega sistema zahteva podjetje. To so zaupnost, celovitost in razpoložljivost.
Zaupnost pomeni, da posredujemo ali omejujemo dostop do informacij ali informacijskega vira z vidika zaupnosti oziroma ohranjanja tajnosti informacij ali informacijskega vira. Celovitost pomeni, da obstaja možnost ugotavljanje sprememb v informacijah in obstoj kontrol, ki so potrebne za zaščito celovitosti informacij ali informacijskih virov. Razpoložljivost pomeni, da so informacije ali nek informacijski vir na voljo takrat, kadar jih potrebujemo. [3]

V današnjih časih se informacijski sistem zelo spreminja. Vse več je nevarnosti, ki grozijo sistemu, zato je pomembno, da se varnostna politika spreminja in tako prilagaja obstoječemu sistemu varnosti. Prav tako je za vsako podjetje varnostna politika drugačna in ima drugačne specifične lastnosti in potrebe po varnosti. Zato poznamo več različnih pristopov k izdelavi ustrezne varnostne politike. Ko podjetje vpelje varnostno politiko je pomembno, da jo ustrezno posodablja in dopolnjuje glede na spremembe v podjetju in nenehen tehnološki razvoj, ki prinaša številne spremembe.

Ker varnostna politika zajema širok spekter na področju varovanja informacij, lahko varnostno politiko delimo na več različnih elementov, ki se upoštevajo pri izdelavi varnostne politike izbranega informacijskega sistema. Nekateri elementi varnostne politike so: [3]

- 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, ozaveščanje, 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.

Z uveljavo varnostne politike lahko podjetje dokazuje ustreznost in nivo zaščite informacij in skladnost z zakonodajo. Podjetje lahko tako na osnovi varnostne politike izpolnjuje pogoje za pridobitev certifikata po standardu ISO 27001. Standard je lahko v veliko pomoč pri usmerjanju pisanja in zajemanja pomembnih elementov varnosti.

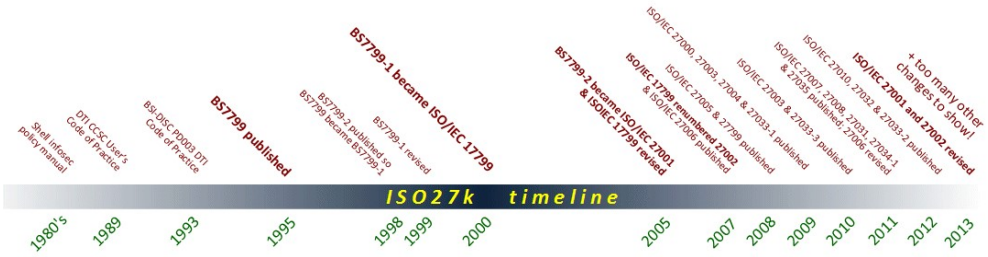
Slika 3.1: ISO 27001 Certification. [12]

Poglavje 4

Standardi na področju informacijske varnosti

Različni standardi nam v življenju lahko zelo pomagajo na vseh področjih. Dajejo nam neke smernice, po katerih se ravnamo in tako izdelki in storitve postanejo bolj učinkoviti in zanesljivejši. Danes poznamo več različnih standardov, postopkov, dobrih praks in metodologij, ki zagotavljajo uspešno varovanje informacij.

V nadaljevanju bom na kratko opisal družino standarda, ki je namenjen za vse organizacije. To so standardi serije ISO/IEC 27000. V preteklosti so kot temeljni standard svetovne organizacije za varovanje informacij prevzele Britanski standard BS 7799. Razvoj standarda BS 7799 sega v leto 1987, prvi objavljeni dokumenti so bili leta 1989, leta 1995 pa je bil prvi sprejeti standard BS 7799:1995. Leta 1999 je bil sprejet posodobljeni standard BS 7799:1999. Ta standard je bil z manjšimi spremembami 1. decembra 2000 sprejet kot standard ISO 17799:2000. Nadaljnji razvoj standarda je bil narejen leta 2002, ko je bil sprejet britanski standard BS 7799-2:2002. [3]



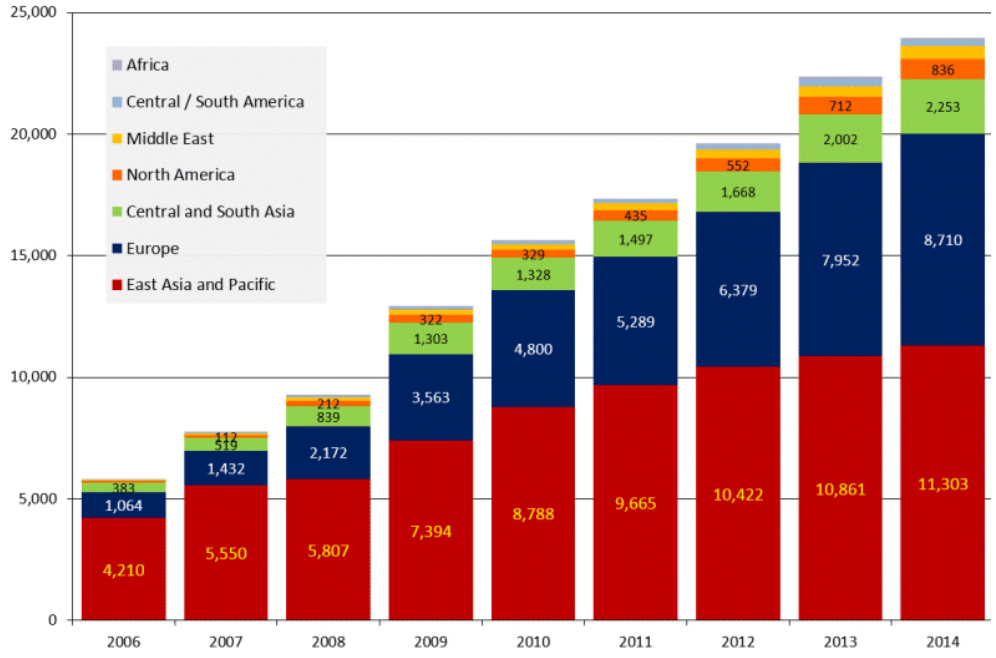
Slika 4.1: Časovnica razvoja družine standarda ISO 27000. [13]

Standard BS 7799 je sestavljen iz dveh delov. Prvi del, ISO/IEC 17799:2000, predstavlja najboljšo prakso za zadovoljevanje zahtev standarda in predlaga, kaj naj bi organizacija imela, drugi del, BS 7799-2:2005, pa je specifikacija – zbirka lastnosti, ki jim mora sistem upravljanja ustrezati, da bo skladen s standardom. Kasneje se je le-ta razdelil na BS 7799-1 in nato na BS 7799-2. [8]

Leta 2005 se je iz BS 7799-1 razvil standard ISO/IEC 17799 (27002) in iz BS 7799-2 standard ISO/IEC 27001. Tako se je standard BS 7799 razvil v družino mednarodnih standardov ISO/IEC 27000, ki imajo mednarodno veljavo in je poznan kot ISMS družina, ki predstavlja najboljše prakse in navodila za vodenje informacijske varnosti, tveganjih in nadzoru v okviru ISMS. [5]

Družina standardov ISO 27000 predstavlja garancijo varovanja informacij v okviru organizacije za poslovne partnerje, ki prinaša poslovne koristi. Pri vpeljavi standarda spoznamo težave in tveganja informacijske varnosti in jih zmanjšamo na minimalen nivo nevarnosti. Ko spoznamo tveganje, se tako lahko osredotočimo na učinkovito rešitev. Ta standard je najmočnejši z vidika informacijske varnosti. Omejen je le s procesnega vidika.

Standard ISO 27001 se bolj osredotoča na vlogo managementa pri informacijski varnosti. Uporablja se za postavitev temelja oziroma okvira informacijske varnosti v podjetju, medtem ko ISO 27002 določa konkretno implementacijo nadzora in kontrole. [4] Združitev standardov ne bi predstavljala ustrezne rešitve, saj bi dobili en sam preobsežen standard, preveč kompleksen za praktično uporabo. Število certificiranja standarda ISO 27001 vztrajno raste iz leta v leto:



Slika 4.2: Rast uporabe standarda ISO 27001. [13]

Standard ISO 27001 daje napotke kako graditi, upravljati, vzdrževati in izboljševati sistem za upravljanje varovanja informacij (SUVI) v organizaciji. [6] Najnovejša revizija tega standarda je bila objavljena v letu 2013. ISO 27001 se lahko vpelje v kakršni koli organizaciji ne glede na velikost ali poslanstvo. Standard so napisali in definirali najboljši strokovnjaki na svetu na področju informacijske varnosti in določa metodologijo za izvajanje upravljanja varovanja informacij v organizaciji. [9]

Uvedba standarda je proces, ki poteka po naslednjih fazah:

Slika 4.3: Vzpostavitev sistema za upravljanje informacijske varnosti.

Splošna zahteva standarda je, da vodstvo organizacije razvije, izvede, vzdržuje in redno izboljšuje dokumentiran SUVI v skladu s poslovnimi aktivnostmi, ranljivostjo in novostmi na področju groženj in tveganj v organizaciji. Naloga SUVI je, da zagotavlja ustrezne varnostne ukrepe, ki ščitijo informacije in vzbuja varnost in zaupanje strankam in vsem zainteresiranim. Za izvajanje SUVI je v organizaciji odgovorno vodstvo, skrbnik informacijskega sistema in pa vsi zaposleni.

Poglavje 5

Varnostna politika zdravstvenega doma

5.1 Uvod v vsebinski del

Zelo velik napredek na področju računalniške in informacijske tehnologije je pripomogel k večji avtomatizaciji in organiziranosti dela v organizacijah. Poslovanje podjetij, ustanov in organizacij temelji na informacijskih sistemih. Informacija za organizacijo pomeni vrednost, ki jo je potrebno varovati in ustrezno zaščititi, saj je za poslovni uspeh, upravljanje informacij in informacijskega sistema pri poslovanju, lahko posamezna vrednost ključnega pomena.

V petem poglavju je opisana varnostna politika specifičnega zdravstvenega doma, ki bo ostal anonimen. Zdravstveni dom je javni zavod. Vizija zdravstvenega doma je izvajanje zdravstvene dejavnosti na primarni ravni vključno z izvajanjem nujne medicinske pomoči. Za uspešno in učinkovito upravljanje dela pa je zelo pomemben dejavnik nemoteno delo. Poslovanje organizacije temelji na informacijskem sistemu, ki ga je potrebno ustrezno vzpostaviti, varovati in posodabljati.

Zgradba varnostne politike temelji na merilih, ki so za našo organizacijo najbolj primerna. Zgledoval sem se tudi po preteklih izkušnjah, ki so pokazale,

kje pretijo največje nevarnosti in na katerem področju je pomembno, da so zaposleni ozaveščeni o varovanju informacijskega sistema. Zelo pomembno je, da smo se posvetovali z vodstvom organizacije, ki nam je podalo želje in pričakovanja.

Varnostna politika vsebuje pravila na področju informacijskega sistema. Ta pravila so razdeljena po poglavjih, ki smo jih opredelili. Na začetku so vsebovana pravila, ki veljajo na področju razvoja in vzdrževanja informacijskega sistema. Opisan je postopek, ki velja pri nabavi programske in strojne opreme. Programsko in strojno opremo je potrebno tudi ustrezno vpeljati v informacijsko okolje in seznaniti uporabnike z uporabo opreme. V tem poglavju je opisano tudi vzdrževanje in nadgradnja programske opreme ter ostale značilnosti, ki veljajo na tem področju.

Nato sledi poglavje, kjer so opredeljene tehnične zmogljivosti informacijskega sistema. Računalniška oprema, ki se nahaja v organizaciji, ima različno stopnjo razpoložljivosti dostopa na posameznih lokacijah.

V poglavju fizično in okoljsko varovanje informacij so predstavljeni postopki in pravila, ki veljajo v zvezi z varovanjem prostorov objekta in varovanjem računalniške opreme, na kateri poteka informacijski sistem. V današnjem času lahko dostop nepooblaščenih oseb do informacij povzroči hude posledice. Varovanje posameznih območji v organizaciji je različno in zato zahteva različne postopke varovanje območji javnega dostopa, zdravstvih prostorov, upravnih prostorov, računalniško informacijskega sistema in območje komunikacijskega sistema. Zelo pomembno je tudi varovanje računalniške in druge opreme. Pomembno je, da se zagotavlja politika čiste mize, praznega zaslona in ustreznega odstranjevanja podatkov. V primeru incidenta so opisani tudi postopki, po katerih se morajo ravnati zaposleni.

Zelo pomembno poglavje je tudi kontrola dostopa. V poglavju so opisana vsa pravila, ki veljajo za upravljanje in varovanje uporabniških in administratorjevih gesel v informacijskem sistemu, ter o sestavi in principu vzdrževanja gesel. V nadaljevanju je opisan tudi dostop administratorja in dostop uporabnikov do sistema, aplikacij in podatkov. Opisani so postopki evidentiranja

uporabnikov, ki lahko dostopajo do sistema, aplikacij in podatkov. Nadzorovanje dostopa do omrežij se nanaša na dostop do lokalnih omrežij, ki mora biti pod strogim nadzorom. V poglavju so tudi opisana pravila, ki veljajo pri oddaljenem dostopu preko VPN povezave in pa pravila, ki veljajo za zaščito komunikacijskih segmentov omrežja in strežnikov pred zlonamerno kodo.

Poslovanje organizacije dostikrat temelji tudi na povezovanju in delovanju storitev s tretjo stranko. V poglavju upravljanje obratovalnih postopkov in komunikacij so razdelana pravila, ki opredeljujejo, kako je sestavljena pogodba s tretjo stranko, ki lahko dostopa do informacijskega sistema in kakšna so storitve tretje stranke. Pri opisu storitev morajo biti opredeljeni cilji in ravni izvajanja storitev ter način poročanja in doba opravljanja teh storitev. V razdelku nadzora dostopa tretjih strank do informacijskega sistema in informacij je opredeljen fizični in logični dostop teh strank. Zapisana so pravila, v kakšnih primerih lahko dostopajo tretje stranke do aplikacij in podatkov v organizaciji preko informacijska sistema.

Dandanes je zelo pomembno, da imamo v svojem informacijskem sistemu nekakšno dodatno rešitev v primeru izgube podatkov. V ta namen so nam v veliko pomoč kopije podatkov. V poglavju varnostno kopiranje podatkov so zapisana pravila in procedure za izvajanje varnostnega kopiranja podatkov, kje so shranjeni mediji z varnostnimi kopijami in pa preverjanje celovitosti podatkov ter delovanje medija.

Zdravstveni dom ima določene zahteve za sledljivost ob spremembi podatkov in beleženjem revizijskih sledi na informacijski strukturi. Omogočeno mora biti ugotavljanje, kdo je vnesel, ažuriral ali drugače spremenil ali izbrisal kateri podatek in kdaj. Prav tako je omejen čas hrambe osebnih podatkov. Vse to je opisano v poglavju revizijska sled.

V primeru incidenta, ki lahko ogrozi delovanje organizacije, je potrebno ustrezno ukrepati. Zato je zelo pomembno, da seznanimo zaposlene z možnostmi incidentov, ki pretijo organizaciji. V poglavju upravljanje varnostnih incidentov se seznanimo z nezaželenimi in nepričakovanimi dogodki. Skozi postopke spoznamo, kako je potrebno odreagirati in katere osebe moramo obvestiti v

primeru incidenta. To so pravila, ki veljajo v zvezi s prijavo in beleženjem incidenta. Na napakah, ki so se že dogajale, je potrebno incidente rešiti, analizirati in jih seveda v čim večji meri v nadaljnju tudi preprečiti, zato po zaključenem reševanju incidenta pooblaščena oseba oceni posledice incidenta in ukrepe.

Zadnje poglavje je uporaba storitev interneta. Zavedati se moramo, da je uporaba interneta danes v veliki meri zelo pogosta. Internet ali medmrežje je računalniško omrežje, ki povezuje več omrežij. Internet se velikokrat nanaša na storitve kot so svetovni splet, elektronska pošta in neposredni klepet. V poglavju so zapisana pravila, ki določajo, v kakšne namene se lahko uporablja svetovni splet in opozarja na nevarnosti, ki se lahko pojavijo pri uporabi interneta. Vsak uporabnik za službeno pošto uporablja poštni strežnik zdravstvenega doma. V poglavju so zapisana pravila in nevarnosti pri uporabi elektronske pošte.

5.2 Razvoj in vzdrževanje informacijskega sistema

5.2.1 Nabava programske, sistemske in strojne opreme

Nabava programske, sistemske in strojne opreme se v ZD izvaja skladno z letnim planom nabave in po postopku, ki je opredeljen v pravilniku o postopkih naročanja.

Postopek nabave se razlikuje glede na vrednost naročila in se izvede bodisi po postopku zbiranja ponudb bodisi z naročilnico. Nato se izpolni podatke v obrazcu »Predlog izvedbe javnega naročila«. Med obvezne podatke mora vpisati zahtevano funkcionalnost in zmogljivost programske, sistemske in strojne opreme.

Pred nakupom strojne opreme (aparata, stroja, ...) se mora vodja oddelka ali druga odgovorna oseba, ki se dogovarja z dobaviteljem, posvetovati z zunanjim izvajalcem za sistemsko informatiko. Le-ta poda strokovno mnenje o

tem ali načrtovana strojna oprema izpolnjuje pogoje za integracijo v informacijski sistem zavoda. Hkrati pa zunanji izvajalec za sistemsko informatiko sodeluje pri dogovarjanju z dobavitelji strojne opreme.

5.2.2 Namestitev programske, sistemske in strojne opreme

Pravila, ki veljajo pri namestitvi programske in sistemske opreme, so:
Vsa programska in sistemska oprema, ki se nameša v ZD, ustreza zahtevam in pogojem licenčnih predpisov.
Zunanji izvajalec za sistemsko informatiko je odgovoren za spremljanje veljavnosti oziroma poteka licenc in je dolžan sprožiti postopek za nabavo novih licenc, predvsem to velja za antivirusni program, ki se nadgrajuje na letni osnovi.
V zavodu obstaja evidenca veljavnih licenc programske in sistemske opreme, ki se vodi v okviru knjigovodskih evidenc »Register osnovnih sredstev« na kontih nematerialnih pravic. Na računalniški informacijski sistem je dovoljeno le nameščanje odobrene programske in sistemske opreme, ki jo določi in namesti zunanji izvajalec za sistemsko informatiko, ali skrbnik informacijskega sistema. V primeru, da programsko in sistemsko opremo namesti zunanji dobavitelj, se zagotovi nadzor, ki ga opravi zunanji izvajalec za sistemsko informatiko ali skrbnik informacijskega sistema.
Nameščanje druge programske in sistemske opreme brez dovoljenja oziroma vednosti zunanjega izvajalca za sistemsko informatiko ali skrbnika informacijskega sistema je prepovedano in onemogočeno (da bi nepooblaščene osebe nameščale programsko in sistemsko opremo na osebnih računalnikih je zaščiteno z nastavitvami uporabniških pravic v domeni).

Pravila, ki veljajo pri namestitvi strojne opreme, so:
Namestitev strojne opreme, ki vključuje osebne računalnike, monitorje, tiskalnike in čitalce izvaja zunanji izvajalec za sistemsko informatiko, ki po namestitvi preveri delovanje nameščene opreme. Nova strojna oprema se po-navadi implementira in poveže v obstoječi informacijski sistem, ki se uporablja v zavodu. Zaposleni zavoda ne smejo izvesti spremembe na strojni

opremi brez vednosti zunanjega izvajalca za sistemsko informatiko ali skrbnika informacijskega sistema.

5.2.3 Nadzor nad verzijami programske opreme

Vsaka spremenjena verzija programske opreme, ki se nameša v ZD, je enolično označena, da je zagotovljena sledljivost nad verzijami. Oznako verzije programske opreme določi posamezni razvijalec programske opreme (zunanji izvajalec oziroma dobavitelj). Zunanji izvajalec oziroma dobavitelj je odgovoren za vodenje evidence o verzijah programske opreme.

5.2.4 Razvoj programske opreme

Večina faz razvoja programske opreme, ki jo ZD potrebuje in uporablja pri svojem poslovanju, se izvaja pri zunanjih izvajalcih oziroma dobaviteljih programske opreme.
Postopek razvoja programske opreme vključuje naslednje faze:

1. Začetek projekta:
   Izdelavo projektne dokumentacije izvede zunanji izvajalec oziroma dobavitelj. Izdela projektno nalogo, kjer se opredeli:

   - poslovne cilje, ki jih bo izpolnila nova programska oprema,
   - opis zahtevane funkcionalnosti programske opreme,
   - obseg projekta,
   - omejitve in predpostavke na projektu.

2. Izbira zunanjega izvajalca:
   V ZD se izvede izbira zunanjega izvajalca za programsko opremo skladno s »Pravilnikom o postopkih naročanja«.
   V razpisni dokumentaciji se pri pogojih, ki jih mora izpolnjevati zunanji izvajalec oziroma dobavitelj programske opreme na področju zdravstvene dejavnosti, navede tudi zahteve glede sposobnosti izvajalca, da

ustrezno varuje informacije, ki jih izvajalec lahko izkaže s certificiranim sistemom vodenja varovanja informacij ali s kadri s certifikati na področju upravljanja in revidiranja sistemov varovanja informacij.

3. Določitev vlog:
   V okviru projekta se v ZD imenuje vodjo projekta oziroma tako imenovanega ključnega uporabnika (odgovorna oseba na posameznem poslovnem področju) in ostale člane projektne skupine.
   Ključni uporabniki v ZD so:

   - pomočnica direktorice za zdravstveno nego,
   - vodje oddelkov (po posameznih zdravstvenih dejavnostih, vodja računovodstva, vodja oddelka za splošne, kadrovske in gospodarske zadeve).

   Med ostale člane projektne skupine sta vključena skrbnik informacijskega sistema in zunanji izvajalec za sistemsko informatiko. Vodja projekta ima nalogo planiranja in koordiniranja dela sodelujočih pri izvedbi ter poročanja direktorici.

4. Izdelava vzpostavitvenega dokumenta projekta:
   Zunanji izvajalec oziroma dobavitelj programske opreme izdela dokument projekta, ki vsebuje:

   - predstavitev projekta (namen, cilj, predpostavke, omejitve, tveganja),
   - vsebino projekta (prednosti nove programske opreme, tehnične lastnosti, varnostne zahteve),
   - organizacijo projekta (organizacijsko shemo in opis zadolžitev sodelujočih, nadzor projekta: določi se kontrolne točke – pregled terminskega načrta in validacijo razvoja),
   - načrt razvoja (izdelke, terminski načrt z opisom aktivnosti, plan resursov).

5. Izdelava specifikacij:
   Pripravi se tehnični načrt s strani zunanjega izvajalca, kjer se opredeli:

   - potrebne funkcionalnosti,
   - enolične specifikacije elementov programske opreme,
   - varnostne zahteve, ki vključujejo: zahteve ob prijavi, zahteve funkcionalnosti, ki zagotavljajo varnost podatkov v fazi vnosa, obdelave, prenosa in hranjenja (mehanizmi validacije vhodnih in izhodnih podatkov, šifriranje...) in zahteve glede revizijskih sledi,
   - načrt testiranja (priprava običajnih in mejnih testnih primerov).

6. Izvedba razvoja programske opreme:
   Razvoj poteka v razvojnem okolju na računalniški opremi zunanjega izvajalca oziroma dobavitelja programske opreme.
   Vodja projekta – ključni uporabnik v ZD spremlja potek razvoja programske opreme. V primeru neskladnosti z načrtom projekta se v zavodu odloča o spremembi načrta, prekinitvi ali nadaljevanju projekta.

7. Izdelava dokumentacije:
   Zunanji izvajalec oziroma dobavitelj izdela dokumentacijo nove programske opreme, ki vsebuje vsaj:

   - navodilo za namestitev (testne in produkcijske verzije),
   - enolično oznako nove verzije,
   - opis sprememb nove verzije,
   - opis tehničnih zahtev za strojno in programsko opremo strežnika, na katerem bo nameščena nova programska oprema,
   - navodilo za testiranje,
   - uporabniški priročnik.

8. Testiranje:
   Testiranje programske opreme je obvezna faza pred prevzemom.

Prvo, nadaljnjo in prevzemno testiranje izvede zunanji izvajalec oziroma dobavitelj v svojem razvojnem in testnem okolju z namenom odpraviti neskladnosti s specifikacijami programske opreme. Ko se z ustreznim postopkom testiranja ugotovi, da izdelana programska oprema zagotavlja v pogodbi opredeljeno funkcionalnost, zmogljivost in varnostne zahteve, odgovorne osebe pri zunanjem izvajalcu, ki so izvedle testiranja, s podpisom potrdijo zapisnik rezultatov testiranja.

9. Prevzem programske opreme:
   Za prevzem programske opreme z ustrezno dokumentacijo so v ZD odgovorni ključni uporabniki.
   Prevzem programske opreme in pripadajoče dokumentacije v ZD dokazuje podpisan primopredajni zapisnik. Pri prevzemu programske opreme sodelujeta skrbnik informacijskega sistema in zunanji izvajalec za sistemsko informatiko.

10. Namestitev programske opreme v produkcijsko okolje:
    Zunanji izvajalec za sistemsko informatiko in skrbnik informacijskega sistema v sodelovanju z zunanjimi izvajalci skladno z navodili za namestitev in tehnično dokumentacijo namestita programsko opremo.
    V primeru, da zunanji izvajalci samostojno izvedejo namestitev programske opreme, skrbnik informacijskega sistema in zunanji izvajalec za sistemsko informatiko izvajata nadzor in sta fizično prisotna pri nameščanju.

11. Usposabljanje uporabnikov:
    Po namestitvi programske opreme sledi usposabljanje uporabnikov (ključnega uporabnika ali širše skupine uporabnikov nove programske opreme) s strani zunanjega izvajalca in prejem uporabniškega priročnika.

5.2.5 Vzdrževanje programske opreme

V kolikor uporabniki pri delu s programsko opremo naletijo na probleme oziroma napake, jih sporočijo na enak način kot vse ostale probleme in napake

pri delovanju informacijskega sistema. Dolžni so obvestiti skrbnika informacijskega sistema.

5.2.6 Nadgradnja programske opreme

Nadgradnjo programske opreme lahko predlaga vsak uporabnik, pri čemer navede razlog za nadgradnjo in predlaga želeni rok izvedbe.

5.3 Tehnične zmogljivosti informacijskega sistema

5.3.1 Informacijski sistem v prostorih zdravstvenih dejavnostih

Računalniška oprema, ki je v zdravstvenih prostorih, zagotavlja srednjo stopnjo razpoložljivosti. V teh prostorih se uporabljajo klimatske naprave, v kolikor je temperatura prostora nad 25 stopinj Celzija. Računalniška oprema je nameščena na pisalnih mizah. Komunikacijski in električni kabli so speljani po kabelskih kanalih do računalniških naprav.

5.3.2 Informacijski sistem v prostorih uprave

Računalniška oprema, ki je v prostorih uprave, zagotavlja nizko stopnjo razpoložljivosti. Oprema je nameščena na pisalnih mizah. Komunikacijski in električni kabli so speljani po kabelskih kanalih do računalniških naprav.

5.3.3 Informacijski in komunikacijski sistem v prostoru informatike

Računalniška oprema, ki je v prostoru informatike, zagotavlja visoko stopnjo razpoložljivosti. Za uporabo računalniške opreme za obdelavo osebnih podatkov in občutljivih osebnih podatkov se uporablja UPS. V prostoru informa-

tike je nameščena klimatska naprava, ki zagotavlja, da je temperatura zraka med 15-25 stopinj Celzija. Računalniška naprava je zaščitena pred udari električnega toka (prenapetostna zaščita). Računalniška oprema je zavarovana s primernim sistemom za gašenje in obveščanjem o kritičnem dogodku (senzor za dim).

5.4 Fizično in okoljsko varovanje informacijskega sistema

Fizično in okoljsko varovanje vključuje vrsto postopkov in pravil v zvezi z varovanjem prostorov in računalniške opreme v ZD. Varovanje posameznih prostorov v zavodu se razlikuje po tem, v kakšno območje spadajo.

5.4.1 Varovana območja na sedežu zavoda

Območje javnega dostopa

Območje javnega dostopa (čakalnice, hodniki, bolniške sobe...) ni posebej varovano, zato se tu ne sme nahajati računalniška oprema ter se ne hranijo in obdelujejo osebni podatki. Obiskovalci se v ZD nahajajo samo v delovnem času med 6. in 20. uro (od ponedeljka do petka) in od 7. -15. ure (v soboto) za namene uporabe storitev, obiska oziroma zaradi pogodbenih obveznosti. Izjema je služba nujne medicinske pomoči, ki deluje 24 ur in 7 dni v tednu. Po končanem delovnem času zunanji izvajalec na področju varovanja izvede pregled prostorov, hodnikov in vrat. Izven delovnega časa v ZD zunanji izvajalec na področju varovanja zagotovi evidenco o obiskovalcih, ki vstopajo v ZD (ne velja za službo nujne medicinske pomoči).

Območje zdravstvenih prostorov

V zdravstvenih prostorih se nahaja računalniška oprema in se hranijo ter obdelujejo osebni podatki. Dostop do posameznih (prenovljenih) zdravstvenih

prostorov je urejen s kontrolo dostopa slepa kljuka, v ostalih zdravstvenih pisarnah je dostop urejen s ključi. S ključem pa je dodatno urejen dostop v posamezne oddelke zdravstvene dejavnosti (ambulanto, dispanzer,...). Ključi za posamezne zdravstvene prostore in ključi vrat oddelkov zdravstvene dejavnosti se hranijo v sprejemni pisarni in v prostoru nujne medicinske pomoči. Zaposleni v sprejemni pisarni in v prostoru nujne medicinske pomoči na podlagi poznavanja zdravstvenega osebja izročijo ključe. Po končanem delovnem času zunanji izvajalec na področju varovanja preveri, ali so vrata v posamezne oddelke zdravstvene dejavnosti zaklenjena. Zdravstveni prostori v službi nujne medicinske pomoči in Centru za preprečevanje in zdravljenje odvisnosti od prepovedanih drog so izven delovnega časa nadzorovani z video nadzorom.

Območje upravnih prostorov

V prostorih uprave (pisarne uprave v tretjem nadstropju, pisarna ekonomata v tretjem nadstropju, sejna soba v tretjem nadstropju, arhivski prostor v kleti, prostor vzdrževalcev v kleti, sprejemna pisarna) se nahaja računalniška oprema in se hranijo ter obdelujejo osebni podatki. Dostop do prostorov uprave je v ZD urejen s kontrolo dostopa ključi. Posamezne prostore po končanem delovnem času zaklenejo posamezni zaposlenih, s ključem pa je dodatno urejen dostop do pisarn uprave v tretjem nadstropju. Ključi za posamezne prostore uprave in ključi vrat uprave v tretjem nadstropju se hranijo v sprejemni pisarni in tajništvu uprave (dvojnik). Zaposleni v sprejemni pisarni na podlagi poznavanja zaposlenih v upravi izročijo ključe. Po končanem delovnem času zunanji izvajalec na področju varovanja preveri, ali so vrata v pisarne uprave v tretjem nadstropju in ostala vrata prostorov uprave zaklenjena.

Območje računalniškega informacijskega sistema

V prostoru informatike se nahaja računalniška oprema in se hranijo ter obdelujejo osebni podatki.
V ZD je prostor informatike namensko opremljen, nameščena je klimatska

naprava in javljalec požara. Dostop do prostora informatike je urejen s kontrolo dostopa s ključem. Dostop do prostora informatike imajo naslednje pooblaščene osebe:

- skrbnik informacijskega sistema,
- zunanji izvajalec za sistemsko informatiko,
- referent v plansko-analitski službi.

Ključ se hrani v prostoru uprave – Fakturiranje in Informatika. Dostop ostalih zaposlenih v prostor informatike je možen le v spremstvu navedenih pooblaščenih oseb. Po končanem delovnem času zunanji izvajalec na področju varovanja preveri, ali so vrata v prostor informatika zaklenjena.

Območje komunikacijskega sistema

Območje komunikacijskega sistema (komunikacijske omare, komunikacijski vodi...), ki je namenjeno prenosu komunikacij, se nahaja v prostoru informatike. Vsa komunikacijska oprema se nahaja v zaklenjeni omari. Ključ do komunikacijske omare se hrani v prostoru informatike. Dostop do omare, kjer se hrani komunikacijska oprema, imata zunanji izvajalec za sistemsko informatiko in skrbnik informacijskega sistema. Komunikacijski vodi so zaščiteni pred prestrezanjem komunikacij. Komunikacijski kabli so nameščeni v ustrezne kanale. Vsi mrežni priključki, ki niso v uporabi, so neaktivni.

5.4.2 Varovanje računalniške in druge opreme

Zagotavljanje čiste mize

Zaposleni ne smejo puščati nosilcev podatkov kot so fizični izvodi in elektronski izvodi z osebnimi podatki na pisarniških mizah ali drugih mestih, kjer so dostopni nepooblaščenim osebam.
Nosilce podatkov – fizične izvode morajo zaposleni varno shraniti po končanem delovnem času in takrat, ko dlje časa niso fizično prisotni v prostoru.

Fizični izvodi - zdravstveni kartoni se morajo hraniti v kartotečni omari v posamezni ambulanti in v skupnih prostorih, namenjenih za arhiviranje.
Fizični izvodi - dokumentacija v prostorih uprave se mora hrani v omarah, ki so opremljene s ključem. Po končanem delovnem času se dokumentacija pospravi v omare, te pa se zaklene.
Nosilce podatkov (elektronske izvode), ki so povezani s podatki iz mamografa in rentgena, morajo zaposleni varno shraniti v omaro po končanem delovnem času ali če dlje časa niso fizično prisotni v prostoru.
Računalniška oprema je fizično varovana s kontrolo dostopa s ključem in programsko varovana s kontrolo dostopa gesel oziroma izklopom računalniške opreme.

Zagotavljanje praznega zaslona

Na računalniške zaslone je večinoma onemogočen vpogled nepooblaščenim osebam (zunanjim obiskovalcem, uporabnikom storitev,...). Vpogled na računalniški zaslon pa lahko v posameznih primerih dovolijo zaposleni, če gre za obdelavo podatkov o uporabniku zdravstvenih storitev, ki mora imeti vpogled v svoje osebne podatke. Ob odhodu zaposlenega z delovnega mesta mora le-ta vključiti ohranjevalnik zaslona in zakleniti računalnik. V kolikor je odsotnost zaposlenega z delovnega mesta večja od 5 minut, se ohranjevalnik zaslona avtomatično vključi, računalnik pa samodejno zaklene. Ob koncu delovnega časa se morajo zaposleni odjaviti iz sistema in aplikacij ter ugasniti osebne računalnike (izklop).

Zagotavljanje ustreznega odstranjevanje podatkov

Zaposleni nosilcev podatkov (USB ključe, zdravstvene kartone, ostalo zdravstveno dokumentacijo, dokumentacijo v upravi) ne smejo odmetavati v koše za smeti. Vsi nosilci podatkov z osebnimi podatki se morajo uničiti na način, ki onemogoči branje vseh ali dela uničenih podatkov.
Fizični nosilci podatkov se uničijo s pomočjo rezalnikov, ki se nahajata v tajništvu uprave in v prostoru obračuna plač.

Pri odstranjevanju podatkov iz elektronskih nosilcev podatkov je prisoten zunanji izvajalec za sistemsko informatiko ali skrbnik informacijskega sistema. Uničeni elektronski nosilci podatkov se oddajo v ekonomat, kjer se zavedejo v evidenco.
V času rednega letnega popisa sredstev se določi odpis posameznih elektronskih nosilcev podatkov, ki je zaveden v komisijskem zapisniku o uničenju le-teh (skladno s pravilnikom o popisu sredstev in obveznosti). Uničeni elektronski nosilci podatkov se odpremijo v podjetje, kjer se izvede reciklaža. Skrbnik informacijskega sistema hrani dokumentacijo kot dokazilo o izvedeni reciklaži.

Postopek proti zlorabi računalniške opreme

Računalniška oprema (osebni računalniki, monitorji, tiskalniki, čitalci) se uporablja samo za službene namene v prostorih ZD, izjema so prenosni računalniki. Pri rednem letnem popisu sredstev se ugotavlja pravilnost dejanskega stanja sredstev (vključno s stanjem računalniške opreme) glede na knjigovodsko stanje.
Za fizično nameščanje in premeščanje računalniške opreme (osebni računalniki, monitorji, tiskalniki, čitalci) je zadolžen zunanji izvajalec za sistemsko informatiko ali skrbnik informacijskega sistema. Nameščanje računalniške opreme se izvede na podlagi obrazca »Zahtevek za namestitev računalniške opreme«, ki ga zunanji izvajalec za sistemsko informatiko prejme od skrbnika osnovnih sredstev.
Zahtevek za namestitev računalniške opreme podajo naslednje pooblaščene osebe:

- pomočnica direktorice za zdravstveno nego,
- vodje oddelkov,
- strokovni vodja.

Obrazec »Zahtevek za namestitev računalniške opreme« vsebuje naslednje podatke:

- osebo, ki je podala zahtevek za namestitev,
- inventarno številko osnovnega sredstva,
- lokacijo (nova),
- datum namestitve,
- podpis osebe, ki je izvedla namestitev.

Zahtevek za premestitev računalniške opreme podajo naslednje pooblaščene osebe:

- pomočnica direktorice za zdravstveno nego,
- vodje oddelkov,
- strokovni vodja.

Obrazec »Zahtevek za premestitev računalniške opreme« vsebuje naslednje podatke:

- osebo, ki je podala zahtevek za premestitev,
- inventarno številko osnovnega sredstva,
- lokacijo (stara, spremenjena),
- datum prenosa,
- podpis osebe, ki je izvedla premestitev.

Vsaka predaja ali sprejem računalniške opreme se evidentira v Register osnovnih sredstev v poslovno-računovodski aplikaciji s strani skrbnika osnovnih sredstev.

5.5 Kontrola dostopa

5.5.1 Upravljanje gesel

Upravljanje in varovanje uporabniških gesel

Geslo uporabnika sistema je namenjeno samo njegovi uporabi, zato so uporabniki sistemov (zaposleni v ZD) odgovorni za vse akcije, ki se zgodijo z uporabo njihove identitete. Gesla uporabniki sistemov ne smejo imeti na vidnem mestu, tako da je onemogočeno nepooblaščeno ravnanje. Uporabniki s svojimi osebnimi gesli ravnajo kot z zaupnimi informacijami in jih ne smejo razkrivati oziroma posojati drugim osebam.
Če zaposleni zasledijo malomarno ali zlonamerno ravnanje z gesli, morajo to takoj sporočiti nadrejenemu. Če obstaja sum razkritja gesla, ga mora uporabnik takoj spremeniti in o tem obvestiti skrbnika informacijskega sistema. Le-temu posreduje zahtevek za menjavo gesla (bodisi gesla na domeni ali za gesla v aplikaciji) v obliki elektronskega sporočila ali telefonsko.
Pri izbiri in menjavi gesel so uporabniki (zaposleni v ZD) dolžni upoštevati naslednja pravila:

- izbirati je potrebno gesla z najmanj 8 in največ 15 znaki,
- geslo je sestavljeno iz najmanj 3 različnih znakov, od katerih je vsaj ena črka ali simbol,
- gesla ne smejo vsebovati šumnikov,
- gesla je potrebno menjati vsakih 6 mesecev,
- ko uporabnik menja geslo, se le-ta 5-krat zapovrstjo ne sme ponoviti.

Upravljanje in varovanje administratorskih gesel

Pri izbiri in menjavi gesel sta skrbnik informacijskega sistema in zunanji izvajalec za sistemsko informatiko dolžna upoštevati naslednja pravila:

- administratorska gesla imajo vsaj 14 znakov,

- gesla vsebujejo velike in male črke, števila in simbole,
- gesla ne smejo vsebovati šumnikov,
- gesla se morajo menjati na 90 dni,
- ko administrator menja geslo, se le-ta 5-krat zapovrstjo ne sme ponoviti.

Vsa administratorska gesla sistemov in aplikacij se shranijo v zaprtih kuvertah v blagajni za nujne primere, da se zagotovi možnost dostopa do sistemov tudi v odsotnosti skrbnika informacijskega sistema in zunanjega izvajalca za sistemsko informatiko. V primeru nujnega posega se mora odprtje katerekoli kuverte z gesli, zabeležiti v obrazec »Evidenca dostopa do administratorskih gesel«.
Evidenca vsebuje naslednje podatke:

- katera odgovorna oseba (direktorica, pomočnica direktorice za zdravstveno nego, strokovni vodja) odobri odprtje kuverte,
- datum in čas odprtja kuverte z geslom,
- kdo je odprl kuverto,
- kdo je dostopal do gesla.

Geslo mora skrbnik informacijskega sistema ali zunanji izvajalec za sistemsko informatiko v najkrajšem možnem času spremeniti.

5.5.2 Upravljanje dostopa

Dostop administratorja do sistema

Na sistemu obstaja en administratorski račun, katerega geslo je hranjeno in namenjeno za posege v nujnih primerih. Skrbnik informacijskega sistema in zunanji izvajalec za sistemsko informatiko imata vsak svoj uporabniški račun, ki ima administratorske pravice.

Dostop uporabnikov do sistema, aplikacij in podatkov

Dostop do sistema, aplikacij in podatkov je omejen s sistemom avtentikacije. V zavodu se izvaja z uporabo uporabniških imen in gesel. Uporabljajo se posamične dostopne pravice (digitalna potrdila in gesla).
Uporabnik se mora pred delom prijaviti v sistem in aplikacijo, po uporabi pa se mora iz nje odjaviti. Sistem omogoča samodejno zaklepanje po 10 minutah neaktivnosti uporabnika. Pravice dostopa do sistema, aplikacij in podatkov se uporabniku določijo glede na vlogo in delovno mesto. Odobrene in dodeljene pravice uporabniku omogočajo, da dostopa do sistema, aplikacij in podatkov, ki jih potrebuje za izvajanje svojega dela.
Pri delu urgence se uporabljajo skupinske dostopne pravice (na domeni – eno uporabniško ime in geslo). Sistem omogoča naknadno ugotavljanje, kdo so bili člani določenega tima v določenem času. Skupinske dostopne pravice so omejene, in sicer tako, da se lahko dostopa le do osebnih podatkov uporabnikov zdravstvenih storitev na določenem oddelku.
Dodelitev in ukinitev pravic dostopa do sistema, aplikacij in podatkov poteka po naslednjem postopku:

a) Vodje oddelkov in pomočnica direktorice za zdravstveno nego posredujejo vodji oddelka za splošne, kadrovske in gospodarske zadeve informacijo o:

   - novem delavcu,
   - premestitvi obstoječega delavca,
   - delavcu, ki ni več v delovnem razmerju.

b) Vodja oddelka za splošne, kadrovske in gospodarske zadeve izpolni in posreduje obrazec na elektronski naslov.
   V obrazec se v okviru **sklopa A** (za zdravnike in zdravstveno osebje) navedejo naslednji podatki:

   - IVZ šifra zdravstvenega delavca,
   - ime in priimek,

- delovno mesto,
- naziv aplikacije, do katere dostopa.

V okviru **sklopa B** (za zaposlene na upravnem področju) se navedejo naslednji podatki:

- ime in priimek,
- delovno mesto,
- naziv aplikacije, do katere dostopa.

V okviru **sklopa C** (za zdravnike, zdravstveno osebje in zaposlene na upravnem področju) se navedejo naslednji podatki:

- ime in priimek zaposlenega, ki se mu ukinejo pravice dostopa,
- datum ukinitve pravic dostopa,
- do katerih aplikacij in podatkov se ukine dostop.

Dodatno vodja oddelka za splošne, kadrovske in gospodarske zadeve v elektronskem sporočilu navede tudi podatke o nazivu oddelka zaposlitve in datumu potrebne izvedbe.

c) Po prejemu obrazca skrbnik informacijskega sistema in zunanji izvajalec za sistemsko informatiko izvedeta naslednje aktivnosti:
Dostop do sistema
Skrbnik informacijskega sistema in zunanji izvajalec za sistemsko informatiko vzpostavita delovanje osebnega računalnika po predpisanih standardih operacijskega sistema. Izvede se priklop osebnega računalnika na domenski strežnik, uporabniku se dodeli uporabniško ime (sestoji se iz naziva ambulante in številk) in geslo.
Dostop do aplikacij in podatkov
Skrbnik informacijskega sistema dodeli zaposlenim v sodelovanju z zunanjimi izvajalci posameznih aplikacij zahtevane pravice dostopa do aplikacij in podatkov. Skrbnik informacijskega sistema po izvedenih aktivnostih

izpolni obrazec in ga posreduje vodji oddelka za splošne, kadrovske in gospodarske zadeve.
Obrazec vsebuje naslednje podatke:

- ime in priimek zaposlenega,
- uporabniško ime (dostop do sistema),
- geslo (za dostop v sistem),
- elektronski naslov,
- okolje, v katerem deluje,
- uporabniško ime (za dostop v aplikacijo in do podatkov),
- geslo (za dostop do aplikacij in podatkov),
- datum dodelitve.

Uporabniki prejmejo obrazec, v katerem so opisane pravice dostopa uporabnika do sistema, aplikacij in podatkov. Obrazec morajo hraniti na varnem mestu, tako da je zagotovljena varnost pred dostopom nepooblaščenih oseb.

d) Novega uporabnika na delovnem mestu, ki ima dodeljeno pravico uporabe osebnega računalnika in dodeljene pravice dostopa do sistemov, aplikacij in podatkov, se evidentira v evidenco, ki vsebuje naslednje podatke:

- lokacija v ZD,
- tip računalnika,
- inv. številka,
- tip ekrana,
- inv. številka,
- tip tiskalnika,
- inv. številka,
- tip čitalca,

- inv. številka,
- IP številka,
- domena,
- uporabniške pravice,
- workgroup
- ime računalnika,
- opis računalnika,
- uporabniško ime,
- geslo,
- e-naslov,
- naložena programska opreme,
- ostalo.

Poleg podatkov v navedeni evidenci so podatki o novem uporabniku in obstoječih uporabnikih, ki uporabljajo aplikacije. Evidenca v aplikaciji omogoča pregled in izpis naslednjih podatkov:

- ime in priimek,
- delovno mesto,
- uporabniško ime.

e) Zaposlenemu se lahko v času njegove zaposlitve v zavodu pravice dostopa omejijo oziroma se mu dodelijo še dodatne pravice. Predlog omejitve in dodatne dodelitve poteka po zgoraj opisanem postopku.

5.5.3 Nadzor dostopa do omrežja

Nadzor dostopa do omrežja se nanaša na nadzor dostopa do lokalnih omrežij ZD. Dostop v lokalno omrežje je mogoč tako z neposredno priključitvijo kot tudi z uporabo posameznih tehnologij za oddaljeni dostop kot je VPN. V

primeru lokalnega dostopa to pomeni strog nadzor nad aktivnimi vrati priključnih stikal, ki so aktivna samo na področjih nadzora. Beleženje administrativnih oddaljenih dostopov se v ZD evidentira in hrani v tako imenovanih log datotekah. Nadzor nad oddaljenimi dostopi zunanjih izvajalcev izvajata zunanji izvajalec za sistemsko informatiko in skrbnik informacijskega sistema.

5.5.4 Oddaljen dostop

Oddaljen dostop do lokalnega omrežja ZD zaposlenim ni omogočen. Do lokalnega omrežja uporabniki z oddaljenih lokacij dostopajo preko VPN povezave, ki se zaključuje na požarni pregradi ZD. Uporabniki so dolžni pri oddaljenem dostopu zagotoviti varnost informacij oziroma preprečiti možnost nepooblaščenega dostopa do notranjega omrežja in podatkov, zato računalniške opreme z vklopljeno VPN povezavo ni dovoljeno puščati nenadzorovane. Na požarni pregradi se beležijo vsi administrativni dostopi zunanjih izvajalcev informacijskih storitev. Na kritičnih strežnikih in aplikacijah pa se beležijo vsi dostopi, s čimer se zagotovi ustrezne revizijske sledi.

5.5.5 Zaščita pred zlonamerno programsko opremo

Pravila, ki veljajo za zaščito komunikacijskih segmentov omrežja in strežnikov pred zlonamerno kodo in njenim nenadzorovanim razširjanjem, so:
ZD uporablja lastno programsko opremo za zaščito pred virusi in drugo neželeno programsko opremo. Omenjena programska oprema je nameščena pri vseh uporabnikih. Uporabljena programska oprema za zaščito pred zlonamerno programsko opremo se redno posodablja, prav tako pa se redno izvaja pregledovanje trdih diskov. Zagotovljena je omejitev neposrednih administrativnih dostopov iz uporabniških v strežniške dele omrežja.

5.6 Upravljanje obratovalnih postopkov in komunikacij

5.6.1 Pogodbeno urejanje razmerij s tretjimi strankami

Pogodba o izvajanju storitev, ki jo izvaja tretja stranka, mora opredeljevati opis storitev in predvideni rok trajanja, oziroma dobo opravljanja teh storitev. Pri opisu storitev morajo biti opredeljeni cilji in vnaprej določene ravni izvajanja storitev, način poročanja ter pravica nadzora pogodbenih obveznosti, lahko tudi s strani tretjih strank.
Pravila, ki veljajo glede pogodbenega urejanja razmerij s tretjimi strankami, so:
Določila o spoštovanju varnostnih zahtev za tretje stranke, ki jih določajo varnostne politike ZD so vključena v pogodbo ali pa so samostojna priloga le-te. Pogodba predstavlja pravno podlago za dostop tretje stranke do določenih podatkov oziroma informacijskega sistema. V pogodbi so vključena določila, da se tretje stranke, ki zagotavljajo storitve in imajo dostop do informacij ali informacijskega sistema, obvezujejo, da osebnih in internih informacij ne bodo posredovale drugim osebam ter da jih bodo varovale tako, da bo preprečeno nepooblaščeno razkritje ter jih ne bodo uporabljale na kakršenkoli način, izven načina, dogovorjenega s pogodbo, v času trajanja te pogodbe in v določenem roku po njenem preteku. V primeru ko tretje stranke obdelujejo osebne podatke, zlasti občutljive osebne podatke, morajo to izvajati v skladu z določili Zakona o varstvu osebnih podatkov in ostalih predpisov, ki urejajo to področje. Pri tem se skladno s pogodbo izvaja varovanje skozi celotno obdobje sodelovanja in pa določeno obdobje po zaključku sodelovanja s tretjo stranko.
V pogodbo s tretjo stranko so vključena določila, ki se nanašajo na:

- način poročanja ter obveščanja o varnostnih incidentih,

- postopke za zaščito sredstev za izvajanje storitev,

- zahteve glede varovanja podatkov ZD,

- nadzor dostopa, vključno z dovoljenimi metodami dostopa tretje stranke,

- vodenje in dostopnost seznama izvajalcev, pooblaščenih za izvajanje storitev,

- obveznosti glede namestitve in vzdrževanja strojne in programske opreme tretje stranke ter zahtevanih fizičnih in logičnih nadzornih mehanizmov dostopa do sistemov, storitev in informacij,

- zahteve, da tretja stranka omrežje varuje pred grožnjami iz zunanjih omrežij z opremo, ki zagotavlja največjo možno varnost pred zlonamerno programsko opremo in zunanjimi vdori do sistemov, storitev in podatkov,

- zahteve, da bo ZD na pisno zahtevo posredoval vse podatke, ki so v zvezi z zagotovitvijo varnosti sistemov, storitev in informacij za izvajanje storitev,

- pravico do revizijskega pregleda (ZD si pridržuje pravico do preverjanja ravni varnosti, ki ga zagotavlja tretja stranka, z varnostnimi pregledi informacijskega sistema tretje stranke),

- možnost vključitve podizvajalcev,

- načine zagotavljanja, da se vse osebe, ki so povezane z zunanjim izvajanjem storitev, vključno s podizvajalci, zavedajo svojih obveznosti glede zagotavljanja ustrezne varnosti.

V pogodbo se vključi tudi določbe, ki določajo ukrepe v primeru kršitev obveznosti iz pogodbe.

5.6.2 Upravljanje sprememb pogodbenih storitev tretjih strank

Spremembe v zvezi z zagotavljanjem pogodbenih storitev se upravlja tako, da skrbnik pogodbe v rednih časovnih intervalih preverja delo tretje stranke. Skrbnik pogodbe je odgovoren za:

- informiranje tretje stranke o relevantnih določbah varnostne politike ZD,

- nadzor in spremljanje ravni izvajanja storitev in varovanja informacij tretje stranke,

- pregledovanje poročil in zapisov tretje stranke,

- spremljanje sprememb pri izvajanju storitev in po potrebi sprožitev postopka za spremembo postopkov oziroma dokumentov varnostne politike in revizijo pogodbe s tretjo stranko.

5.6.3 Nadzor dostopa tretjih strank do informacijskega sistema in informacij

Dostop tretjim strankam do informacij in informacijskega sistema ni dovoljen, dokler niso implementirani ustrezni varnostni in nadzorni mehanizmi ter ni stopila v veljavo pogodba, ki definira pogoje dostopa. Tretjim strankam je omogočen dostop samo do tistih informacij, mrežnih servisov, strežnikov in mrežnih virov v notranjem omrežju, ki jih nujno potrebujejo pri svojem delu. Tretje stranke je potrebno pred začetkom dela seznaniti z varnostnimi politikami, ki jih je tretja stranka dolžna upoštevati. Pogoji sodelovanja in ukrepi nadzora so zapisani v pogodbi med tretjo stranko in ZD. S podpisom pogodbe se tretja stranka obveže spoštovati in upoštevati varnostne predpise in varovati vse podatke, do katerih imajo dostop.

Logični dostop do informacijskega sistema in informacij

Vodja oddelka oziroma druga odgovorna oseba poskrbi, da tretja stranka podpiše izjavo o varovanju podatkov. Za odobritev in izvedbo postopka za dostop tretje stranke v omrežje je potrebno izpolniti naslednje podatke v obrazcu:

- osebne podatke kontaktne osebe tretje stranke (ime, priimek, telefonska številka),
- morebitne časovne omejitve dostopa,
- način dostopa,
- namen oddaljenega dostopa (do katerih mrežnih virov in mrežne opreme potrebuje dostop),
- tehnične podatke (IP številka).

Skrbnik informacijskega sistema ali zunanji izvajalec za sistemsko informatiko pregledata zahtevek in ga po potrebi dopolnita s parametri. Nato določita gesla za dostop tretje stranke skladno z navedbami v zahtevku. Vsi dostopi tretjih strank do informacijskega sistema se beležijo ves čas sodelovanja.
Tretja stranka podpiše obrazec in s tem potrdi prevzem gesel ter da je seznanjena z varnostnimi pravili dostopa. Obrazec se arhivira pri skrbniku informacijskega sistema.
Tretjim strankam se mora prekiniti dostop v omrežje takoj, ko dostopa do informacijskega sistema ne potrebujejo več, oziroma najkasneje ko preneha pogodbeno razmerje med ZD in tretjo stranko.
Čas prekinitve dostopa za tretjo stranko mora vodja oddelka oziroma druga odgovorna oseba sporočiti skrbniku informacijskega sistema ali zunanjemu izvajalcu za sistemsko informatiko. Če je že vnaprej znano, da bo dostop omogočen za določeno dobo, se predviden datum prekinitve dostopa napiše že v obrazec.

Dostop v omrežje se prekine v primeru kršitve določil varnostnih predpisov in navodil. Če se pojavi sum kršitve varnostnih predpisov in navodil, se dostop v omrežje začasno onemogoči, dokler se ne ugotovi dejanskega stanja kršitve.

Fizični dostop do informacijskega sistema in informacij

Obiskovalci ne smejo vstopati in se gibati nenadzorovano po območjih upravnih in zdravstvenih pisarn, pač pa le v spremstvu nekoga od zaposlenih, ki ima pravico dostopa v te prostore. Vzdrževanje opreme lahko izvajajo le pooblaščene tretje stranke, s katerimi je sklenjena pogodba z ustreznimi členi glede varovanja informacij. Izvajalec, ki dejansko opravlja vzdrževalna dela, pa podpiše še sporazum o varovanju informacij.
Skrbnik informacijskega sistema ali zunanji izvajalec za sistemsko informatiko izvajata nadzor dostopa tretje stranke do strojne opreme. Vzdrževalna dela se izvajajo na mestu, kjer se oprema nahaja. Če to ni mogoče, se odstrani nosilec podatkov iz opreme in se ga varno shrani. Če podatkov ni mogoče odstraniti ali kako drugače zaščititi, mora biti postopek vzdrževanja nadzorovan.

5.7 Varnostno kopiranje podatkov

5.7.1 Izvajanje in ravnanje varnostnega kopiranja podatkov

Izbira naprav in medijev za izdelavo varnostnih kopij podatkov ustreza količini podatkov, ki se shranjuje, in zahtevani hitrosti shranjevanja ter restavriranja. Procedure za izdelavo varnostnih kopij podatkov in restavriranje so dokumentirane in zaradi svoje pomembnosti temeljito preizkušene. Mediji za shranjevanje podatkov so ustrezno označeni, da jih je možno v čim krajšem času in pravilno uporabiti pri restavriranju podatkov. Mediji so varno shranjeni tako, da niso dostopni nepooblaščenim osebam. Pooblaščeni osebi za izvajanje varnostnih kopij sta: skrbnik informacijskega sistema in zunanji

izvajalec za sistemsko informatiko. Dnevno se izvaja varnostno kopiranje podatkov na disk za podatke iz programske opreme, ki pokriva zdravstvene dejavnosti.

5.7.2 Shranjevanje prenosnih medijev z varnostnimi kopijami

Prenosni mediji z varnostnimi kopijami podatkov se hranijo v prostoru informatika v ognjevarni omari.
Vsako shranjevanje varnostnih kopij podatkov se evidentira, pri čemer se zabeleži v log datoteki:

- kaj vsebuje varnostna kopija,
- čas izdelave varnostne kopije,
- enolično označbo kopije,
- zapis o uspešnosti in neuspešnosti izdelave kopije.

Označevanje prenosnih medijev z varnostnimi kopijami podatkov vključuje navedbo tedna in dni v tednu (pon-pet). Na medijih se označi tudi datum, ko so bili podatki prvič zapisani na medij.

5.7.3 Preverjanje varnostnih kopij

Zunanji izvajalec za sistemsko informatiko enkrat na 6 mesecev preveri, ali se podatki dejansko nahajajo na označenih prenosnih medijih in da mediji niso poškodovani ali uničeni ter testira, ali bi bilo v primeru incidenta podatke mogoče restavrirati iz varnostnih kopij na prenosnih medijih. Zunanji izvajalec za sistemsko informatiko izvede popolno restavriranje naključno izbranega dela varnostne kopije podatkov. O validaciji varnostne kopije se pripravi zapisnik, ki vsebuje naslednje podatke:

- navedba datuma preveritve varnostne kopije,

- odgovorno osebo, ki je izvedla preveritev,

- rezultat preveritve.

5.8 Revizijska sled

5.8.1 Sledljivost sprememb

ZD ima določene zahteve za sledljivost sprememb nad podatki, beleženjem revizijskih sledi na informacijski infrastrukturi (strežniki, programska oprema, baze podatkov).
Sledljivost sprememb mora biti primerna obdelovanim podatkom in se uporablja za vse osebne podatke (Zakon o varstvu osebnih podatkov), ki se obdelujejo v ZD. Za informacije, ki so označene samo za interno oziroma javno uporabo, sledljivost sprememb ni potrebna.

Prvi nivo sledljivosti velja za osebne podatke in omogoča naknadno ugotavljanje, kdo je vnesel, ažuriral ali drugače spremenil, izbrisal kateri podatek in kdaj. Informacijski sistem v ZD zagotavlja beleženje aktivnosti uporabnika, ki vključujejo vpis, spremembo in izbris posameznega osebnega podatka.

Drugi nivo sledljivosti se uporablja za občutljive osebne podatke in omogoča naknadno ugotavljanje, kdo je vnesel, spremenil ali izbrisal kakšen podatek in kdaj, poleg tega pa se beleži tudi, kdo in kdaj je do določenega podatka zgolj dostopil (vpogled, seznanitev), a podatka ni spremenil. Informacijski sistem v ZD zagotavlja beleženje aktivnosti uporabnika, ki vključujejo vpis, spremembo in izbris ter dostop (vpogled) do posameznega občutljivega osebnega podatka.

5.8.2 Sledljivost sprememb v primeru skupinskih prijav

Pri uporabi skupinske dostopne pravice informacijski sistem v ZD omogoča naknadno ugotavljanje, kdo so bili člani posamezne skupine, sledljivost spre-

memb pa je zagotovljena za nivo obdelovanja osebnih podatkov ali občutljivih osebnih podatkov.

5.8.3 Hramba podatkov o vpogledih v osebne podatke in občutljive osebne podatke

Podatki o dostopih (vpogledih) obstaja, so avtentični in dosegljivi v razumljivem času (največ 14 dni) za namene inšpekcijskih postopkov.

5.8.4 Čas hrambe podatkov o vpogledih v osebne podatke in občutljive osebne podatke

Zbirko vpogledov v osebne podatke ali občutljive osebne podatke se lahko uniči šele po preteku zakonskega roka. ZD lahko po petih letih (razen če zakon ne določa drugačnega roka hranjenja) uniči zbirko vpogledov pod pogojem, da vanjo v tem obdobju ni nihče vpogledal.

5.9 Upravljanje varnostnih incidentov

5.9.1 Prijava in beleženje incidenta

Incident predstavlja enega ali več nezaželenih ali nepričakovanih dogodkov, za katere je zelo verjetno, da bodo lahko ogrozili normalno delovanje ZD oziroma zaupnost, celovitost ali razpoložljivost podatkov, do katerih ZD dostopa, jih obdeluje ali hrani.
Nezaželeni ali nepričakovani dogodki so:

I. izguba, uničenje ali zloraba podatkov (podatki v elektronski obliki, papirni dokumenti itd),

II. namerno ali nenamerno poškodovanje ali zloraba računalniškega informacijskega sistema (uničenje ali poškodbe strojne opreme, okužbe z

zlonamerno programsko opremo, vdori v računalniški informacijski sistem),

III. izpad delovanja računalniškega informacijskega sistema ZD (strojna oprema, programska oprema, komunikacije),

IV. kršenje zakonodaje,

V. neupoštevanje določil varnostnih politik.

Pravila, ki veljajo v vezi z prijavo in beleženjem incidentov, so:
Vsi zaposleni in uporabniki informacijskega sistema v ZD so dolžni prijavljati zaznane incidente pooblaščeni osebi (pomočnici direktorice za zdravstveno nego ali osebi v plansko-analitski službi).
Prijavo incidentov zaposleni sporočijo na naslednje načine:

- ustno,
- telefonsko,
- preko elektronske pošte.

Pooblaščena oseba je dolžna beležiti prijavo incidenta v evidenco, ki vsebuje naslednje podatke:

- kaj se je zgodilo,
- kje je bil zapažen incident,
- kdaj je bil zapažen incident,
- kdo je bil prisoten,
- kakšne so posledice in kakšen vpliv ima incident na informacijski sistem.

Pooblaščena oseba je dolžna beležiti vse prijavljene incidente v evidenco in izvajati aktivnosti odprave oziroma zmanjšanja posledic incidentov. Vsi incidenti, ki lahko povzročijo oziroma so povzročili izgubo, uničenje ali zlorabo

podatkov (podatki v elektronski obliki, papirni dokumenti itd.), so takoj sporočeni na Center za informatiko v zdravstvu (CIZ), ki lahko pomaga pri odpravi ali zmanjšanju škode incidenta.
Vsi incidenti, ki lahko povzročijo oziroma so povzročili namerno ali nenamerno poškodovanje ali zlorabo računalniškega informacijskega sistema oziroma izpad delovanja računalniškega informacijskega sistema, so v istem delovnem dnevu oziroma prvi delovni dan po incidentu sporočeni na CIZ. Vsi incidenti, ki bi lahko bili posledica oziroma so posledica kršenja zakonodaje ali neupoštevanja določil varnostnih politik, so sporočeni v rednih poročilih na CIZ. Pooblaščena oseba o vseh incidentih obvešča vodstvo ZD.

5.9.2 Ukrepanje v primeru pojava incidenta

V primeru pojava incidenta je pooblaščena oseba dolžna ustrezno ukrepati. Glede na vrsto incidenta se ukrepi delijo na ukrepanje v primeru:

- izgube, uničenja ali zlorabe podatkov,
- poškodovanja, zlorabe ali izpada delovanja računalniškega sistema,
- poškodovanja v primeru kršenja zakonodaje,
- neupoštevanja varnostnih politik.

V primeru incidentov, ki lahko povzročijo oziroma so povzročili **izgubo, uničenje ali zlorabo podatkov** (podatki v elektronski obliki, papirni dokumenti itd.) se takoj poskrbi za izvajanje ukrepov za zaščito podatkov. Preostale podatke se primerno zaščititi z ustreznimi varnostnimi ukrepi, kar lahko pooblaščena oseba izvede z vsemi strokovno usposobljenimi sodelavci (informatiki, delavci splošnih služb, varnostniki itd.).
Preveri se revizijske sledi dostopov do izgubljenih, uničenih ali zlorabljenih podatkov, da se ugotovi, kdo in kdaj je povzročil izgubo, uničenje ali zlorabo podatkov. Pooblaščena oseba pripravi poročilo po končanem reševanju incidenta. V kolikor izvajalec nima strokovnega osebja za ugotavljanje vzroka

incidenta, to lahko opravi CIZ. Na podlagi odgovora vodstva na poročilo o incidentu se izvede primerne varnostne ukrepe ter uvede sankcije za osebe, odgovorne za incident.

V primeru incidentov, ki lahko povzročijo oziroma so povzročili **namerno ali nenamerno poškodovanje ali zlorabo računalniškega informacijskega sistema oziroma izpad delovanja računalniškega informacijskega sistema**, se poskrbi za primerno zaščito računalniških informacijskih sredstev (prenos sredstev na varno mesto, omejitev dostopa) oziroma ponovno vzpostavitev računalniškega informacijskega sistema. Primarne aktivnosti se izvedejo za vzpostavitev komunikacijskih povezav z omrežjem in delovanje opreme, namenjene za izvajanje zdravstvene dejavnosti. Pooblaščena oseba pripravi poročilo po končanem reševanju incidenta. Na podlagi odgovora vodstva na poročilo o incidentu se izvede primerne varnostne ukrepe ter uvede sankcije za osebe, odgovorne za incident.

V primeru incidentov, ki predstavljajo **direktno kršitev zakonodaje**, se takoj obvesti ustrezne državne institucije (Policija) in v skladu z njihovimi navodili poda vse podatke oziroma preda sredstva, ki so bila uporabljena pri izvajanju prekrška oziroma kaznivega dejanja. Pooblaščena oseba pripravi poročilo po končanem reševanju incidenta. Na podlagi odgovora vodstva na poročilo o incidentu se izvede primerne varnostne ukrepe ter uvede sankcije za osebe, odgovorne za incident.

V primeru incidentov, ki bi lahko bili posledica oziroma so posledica **neupoštevanje določil varnostnih politik**, se zagotovi primerno zaščito podatkov in računalniškega informacijskega sistema ter zabeleži vse značilnosti incidenta. Pooblaščena oseba pripravi poročilo po končanem reševanju incidenta. Na podlagi odgovora vodstva na poročilo o incidentu se izvede primerne varnostne ukrepe ter uvede sankcije za osebe, odgovorne za incident.

5.9.3 Pregledovanje in presojanje incidentov

Po zaključenem reševanju incidenta pooblaščena oseba oceni posledice incidenta in ukrepe, ki so bili izvedeni na podlagi incidenta. Oceni vrsto inci-

denta, število prizadetih uporabnikov, količino izgubljenih, uničenih ali zlorabljenih podatkov, čas trajanja in pogostost pojavljanja.
Pooblaščena oseba ima odgovornost, da ugotavlja, kdo je bil udeležen v posameznem incidentu, v ta namen pa ima pravico do vpogleda v naslednje podatke:

- vsebina elektronske pošte (s privolitvijo osebe, ki ima ta elektronski naslov),

- prometni podatki elektronske pošte,

- prometni podatki dostopa do interneta,

- podatki, ki se nahajajo na računalniški opremi (lokalni disk, USB ključ, strežniška in omrežna infrastruktura itd.) – razen vsebine elektronske pošte,

- revizijske sledi dostopa do podatkov (kdo in kdaj je podatek ustvaril, spremenil, izbrisal oziroma izvedel vpogled vanj),

- podatki nadzornih mehanizmov (logi brez kontaktnih kartic, video nadzor, vpisi v dnevnik dostopov itd.).

Zaposleni so dolžni sodelovati s pooblaščeno osebo, da se incidenti rešijo in da se podatki ustrezno zaščitijo. Pooblaščena oseba o vseh zaključenih reševanjih incidentov obvešča vodstvo ter v rednih poročilih CIZ. Po končanem reševanju incidenta pooblaščena oseba pripravi poročilo, ki ga posreduje vodstvu ter uporabnikom, ki so incident povzročili. Na podlagi ugotovitev poročila lahko vodstvo sprejme primerne ukrepe, ki lahko izboljšajo stanje varovanja informacij, ter uvede sankcije za osebe, odgovorne za incident.

5.10 Uporaba storitev interneta

5.10.1 Uporaba storitev interneta

Internetna povezava ZD je namenjena službeni uporabi. Internetne storitve (elektronsko pošto, svetovni splet) je sprejemljivo uporabljati v zasebne namene le v obsegu, ki ne ovira delovnega procesa in na način, ki ne ogroža varnosti informacij. Uporabniki dostopajo do svetovnega spleta preko drugega ponudnika internetnih storitev.
Zaposlenim v ZD ni dovoljeno:

a) širjenje in dostopanje do žaljivih in nezakonitih vsebin,

b) nalaganje datotek iz nezanesljivih oziroma sumljivih virov,

c) prenašanje programske opreme v nasprotju z licenčnimi pogoji,

d) nezakoniti kopiranje in izraba avtorskih izdelkov.

Dostopanje do določenih URL naslovov je omejeno. Pooblaščena oseba odobri URL naslov, do katerih se tehnično omeji dostop.

5.10.2 Uporaba elektronske pošte

Uporabniki smejo za službeno pošto uporabljati poštni strežnik ZD. Zasebna pošta mora biti shranjena ločeno od službene elektronske pošte. Uporabniki smejo uporabljati poštne predale, za katere so pooblaščeni, in ne smejo omogočiti uporabe poštnega predala nepooblaščenim osebam. Elektronsko pošto in priponke, ki vsebujejo občutljive osebne podatke, se pri pošiljanju v zunanje omrežje šifrira in podpiše z digitalnim potrdilom. V zavodu so v seznamu »Pooblaščene osebe za pošiljanje občutljivih osebnih podatkov« navedene osebe, ki izvajajo šifriranje in podpisovanje z digitalnim potrdilom. Pri posredovanju ali vračanju elektronske pošte morajo uporabniki preveriti, ali je pošta naslovljena na prave naslove. Uporabniki morajo previdno ravnati z elektronsko pošto in priponkami neznanega oziroma sumljivega pošiljatelja.

Tovrstne elektronske pošte se ne odpira, ampak izbriše. Če pa je pošiljatelj znan, sumljiv pa je naslov ali vsebina elektronske pošte, mora uporabnik pri pošiljatelju preveriti izvor elektronske pošte.
Uporabnik ne smejo uporabljati sistema elektronske pošte za:

a) sodelovanje v verižni pošti,

b) širjenje zlonamerne programske opreme,

c) širjenje žaljivih in nezakonitih vsebin,

d) pošiljanje velike količine elektronske pošte (spam) ali priponk z vsebino, ki ni povezana z opravljanjem delovnih nalog,

e) preusmeritev elektronske pošte na drug naslov.

Uporabniki morajo prijaviti varnostni incident, ko protivirusna zaščita odkrije škodljivo kodo in ko obstaja sum, da je elektronska pošta okužena z virusom. Uporabnik mora v takem primeru takoj prenehati z uporabo računalnika in sme nadaljevati, ko je incident rešen.
Ko zaposleni zapustijo ZD, se njihov elektronski naslov ukine. Morebitni pošiljatelji elektronske pošte na ukinjen elektronski naslov prejmejo obvestilo, da naslov ni več aktiven in elektronski naslov osebe, ki je nasledila zaposlenega na tem delovnem mestu.
Pošiljanje in sprejemanje priponk določenega formata se lahko onemogoči zato, da bi zmanjšali možnosti okužbe z zlonamerno programsko opremo (neposredno izvršljive datoteke s končnicami .exe, .bat, .pif).
Največja velikost priponke je omejena, da se prepreči izpad storitve elektronske pošte. Omejevanje elektronske pošte odobrita skrbnik informacijskega sistema in zunanji izvajalec za sistemsko informatiko.
Uporabljajo se mehanizmi za zmanjšanje neželene pošte (zavračanje prve dostave, uporaba črnih seznamov, vsebinsko pregledovanje).

5.10.3 Nadzor prometa na internetu

Informacijski sistem ZD beleži podatke o prometu na internetu, nadzor nad podatki izvaja zunanji izvajalec za sistemsko informatiko. Nadzor nad tem, kako internet uporabljajo zaposleni, se izvaja v primeru zaznanih varnostnih incidentov.

Poglavje 6

Sklepne ugotovitve

V okviru diplomskega dela sem izdelal varnostno politiko za specifično podjetje oziroma organizacijo. V času izdelave sem sodeloval z vodstvom in nekaterimi zaposlenimi. V veliko pomoč so mi bila priporočila, navodila in dobre prakse na področju izdelave informacijske varnosti. Rešitev na področju informacijske varnosti je več. V veliko pomoč mi je bila družina standardov ISO 27000. V njem so zajete aktivnosti in dobre prakse pri upravljanju informacijske varnosti.

Izdelava diplomskega dela se je pričela s preučevanjem literature, standardov in spoznavanjem organizacije. Diplomsko delo je sestavljeno iz dveh delov. V prvem delu je opisana tematika diplomskega dela in pa standardi s področja informacijske varnosti. Zajema pojem informacijske varnosti in dokumenta varnostne politike. Prav tako sem preučil standard ISO 27001, ki mi je bil v veliko pomoč. Postopki varovanja informacij se od avtorja do avtorja razlikujejo, moj namen pa je bil, da sem združil najboljše plati vsakega postopka in si tako ustvaril celotno sliko dokumenta varnostne politike za organizacijo.

V drugem delu pa je bilo potrebno s pomočjo vodstva opredeliti cilj projekta, ki sem si ga zastavil. Do potankosti sem spoznal informacijski sistem, težo informacij, s katerimi razpolaga organizacija, in celotno strukturo organizacije. Sočasno sem tudi preučeval standarde s področja informacijske

varnosti. Literatura, ki sem jo preučil, zajema širok in obsežen vir informacij. Samostojno sem sestavil smernice in opredelil področja, ki so se mi zdela najbolj pomembna za zavarovanje informacij. Nadaljeval sem s prepisom trenutnega stanja in pa izdelavo varnostne politike. Pri izdelavi sem imel popolno podporo vodstva in zaposlenih, ki so mi zelo pomagali, da je izdelava potekala nemoteno in brez večjih težav.

V zaključku sem varnostno politiko uspešno izdelal in jo predal vodstvu. Zelo pomembno je bilo, da sem izdelek tudi predstavil in poudaril stopnjo pomembnosti dokumenta. Ključen dejavnik, da bo dokument dosegel svoj namen, je na vodstvu, da ga predstavi svojim zaposlenim. Vodstvo mora organizirati izobraževanja, na katerih bo razumljivo in enostavno predstavljen zaposlenim. Le tako bomo v popolnosti dosegli cilj varnostne politike podjetja.

Skozi izdelavo diplomskega dela sem se naučil veliko novih in uporabnih stvari. V veliki meri sem spoznal težo varnosti na področju informacijskega sistema in pomen informacije. Dokument varnostne politike ni neko pravilo oziroma postopek, ki bi veljal za vsako organizacijo, ampak se spreminja glede na potrebe in značilnost organizacije. Varnostna politika je v različnih podjetjih različna, primerna glede na velikost le-tega in števila zaposlenih. Ugotovil sem, da dobra varnostna politika lahko zelo pripomore k varnejšemu in bolj organiziranemu delu in predstavlja večjo varnost. Če bi še enkrat izdeloval varnostno politiko, bi se je lotil bolj podrobno in bi morda spremenil kakšen njen segment. Vemo, da se dokument s časoma mora spreminjati in dopolnjevati, zato menim, da ga lahko čez čas, ko ugotovimo pomanjkljivosti, še izdatno dopolnimo in izboljšamo. Tistemu, ki si v svojem podjetju ali organizaciji želi vpeljati varnostno politiko predvsem na informacijski ravni, predlagam, da preuči standarde s področja informacijske varnosti in si na podlagi standardov ter smernic izdela dokument, ki bo pripomogel k varnosti. Dela se mora lotiti premišljeno in seveda mora dodobra poznati zgradbo in strukturno informacijskega sistema v organizaciji ali podjetju.

Literatura

[1] M. Egan, T. Mather, Varovanje informacij: grožnje izzivi in rešitve, 2005 [Dostopano 11. 3. 2016].

[2] D. Trček (2015) Prosojnice s predavanj C pri predmetu: Informacijska varnost in zasebnost. [Online]. Dosegljivo: https://ucilnica.fri.uni-lj.si/course/view.php?id=92 [Dostopano 11. 3. 2016].

[3] M. Štrakl (2003) Varnostna politika informacijskega sistema. [Online]. Dosegljivo: http://lms.uni-mb.si/vitel/14delavnica/. [Dostopano 11. 3. 2016].

[4] R. Kralj (2012) Varnostna politika informacijskega sistema. [Online]. Dosegljivo: http://www.fvv.um.si/konferencaiv/zbornik/Kralj.pdf. [Dostopano 11. 3. 2016].

[5] T. Schweighofer (Diplomsko delo) Vpeljava varnostne politike v srednje velikem podjetju. [Online]. Dosegljivo: https://dk.um.si/IzpisGradiva.php?id=15194. [Dostopano 11. 2. 2016].

[6] D. Košćak (Diplomsko delo) Varovanje informacij v skladu s standardom ISO/IEC 27000. [Online]. Dosegljivo: http://eprints.fri.uni-lj.si/1362/. [Dostopano 11. 2. 2016].

[7] S. Tomažič (Diplomsko delo) Analiza varnosti informacijskega sistema uprave republike Slovenije za jedersko varnost. [Online]. Dosegljivo:

http://diplome.fov.uni-mb.si/vis/13341Tomazic.pdf. [Dostopano 11. 2. 2016].

[8] A. Kočan (Diplomsko delo) Analiza varnosti informacijskega sistema v podjetju STROKA PRODUKT D.O.O. [Online]. Dosegljivo: https://dk.um.si/Dokument.php?id=10918. [Dostopano 11. 2. 2016].

[9] O standardu ISO 27001. [Online]. Dosegljivo: http://www.iso-27001.si/ [Dostopano 19. 9. 2014].

[10] Informacijska varnost. [Online]. Dosegljivo: https://sl.wikipedia.org/wiki/Informacijska_varnost. [Dostopano 19. 9. 2015].

[11] Slovar informatike - islovar. [Online]. Dosegljivo: http://www.islovar.org/iskanje_enostavno.asp. [Dostopano 19. 9. 2014].

[12] ISO 27001 Certification. [Online]. Dosegljivo: http://www.irqs.co.in/blog/tag/iso-27001-certification/page/2/. [Dostopano 19. 9. 2014].

[13] ISO/IEC 27001:2013. [Online]. Dosegljivo: http://www.iso27001security.com/html/27001.html [Dostopano 19. 9. 2014].