UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Katja Rigelnik

Izdelava varnostnih kopij kot varnostni mehanizem za zagotavljanje neprekinjenega poslovanja organizacije

DIPLOMSKO DELO

VISOKOŠOLSKI STROKOVNI ŠTUDIJSKI PROGRAM PRVE STOPNJE RAČUNALNIŠTVO IN INFORMATIKA

Ljubljana 2014

UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Katja Rigelnik

Izdelava varnostnih kopij kot varnostni mehanizem za zagotavljanje neprekinjenega poslovanja organizacije

DIPLOMSKO DELO

VISOKOŠOLSKI STROKOVNI ŠTUDIJSKI PROGRAM PRVE STOPNJE RAČUNALNIŠTVO IN INFORMATIKA

Mentor: viš. pred. dr. Aljaž Zrnec

Ljubljana 2014

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: 00555 / 2013
Datum: 15.9.2013

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

Kandidat: **KATJA RIGELNIK**

Naslov: **IZDELAVA VARNOSTNIH KOPIJ KOT VAROVALNI MEHANIZEM ZA ZAGOTAVLJANJE NEPREKINJENEGA POSLOVANJA ORGANIZACIJE**
BACKUP AS A BUFFER MECHANISM TO ENSURE UNINTERRUPTED OPERATIONS OF THE ORGANIZATION

Vrsta naloge: Diplomsko delo visokošolskega strokovnega študija prve stopnje

Tematika naloge:

V zadnjih letih se informacijska varnost razvija v smeri, ki jo opredeljujejo ISO standardi in tako postavljajo okvir za vzpostavitev mnogih kontrol. Organizacije uvajajo varnostne politike z namenom zagotavljanja neprekinjenega poslovanja. To pomeni, da delujejo v smeri varovanja podatkov, ki imajo bistveno vrednost za njen obstoj in delovanje. Še posebej izpostavite varnostno kopiranje podatkov, saj analize tveganj izdelane na osnovi groženj, kažejo na to, da le-ti nikakor niso varni pred izgubo. V drugem delu predstavite izbrano organizacijo, ki deluje na področju javne uprave, za katero je neprekinjeno delovanje bistvenega pomena. Predstavite kontrole in izzive na področju njihovega varnostnega kopiranja podatkov. Ker je organizacija na razpotju zaradi dotrajanih sistemov, predstavite možnosti realizacije varnostnega kopiranja v oblaku. Na osnovi pregleda obstoječega stanja in ciljev na koncu predstavite smernice, ki bi omogočile sistematično ter učinkovito upravljanje in vzdrževanje sistema za varnostno kopiranje v organizaciji.

Mentor: Dekan:

viš. pred. dr. Aljaž Zrnec prof. dr. Nikolaj Zimic

Fakulteta za računalništvo in informatiko • UNIVERZA V LJUBLJANI • 2

I Z J A V A O A V T O R S T V U

diplomskega dela

Spodaj podpisana **Katja Rigelnik**,

z vpisno številko **63980066**,

sem avtorica diplomskega dela z naslovom:

Izdelava varnostnih kopij kot varnostni mehanizem za zagotavljanje neprekinjenega poslovanja organizacije

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal/-a samostojno pod mentorstvom **viš. pred. dr. Aljaža Zrneca**
- 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 _____ Podpis avtorja/-ice: _____

Zahvaljujem se mentorju viš. pred. dr. Aljažu Zrnecu za pomoč in nasvete pri izdelavi diplomske naloge. Posebna zahvala gre oddelku za informatiko javnega zavoda za svetovanje in strokovno vodenje pri izdelavi diplomskega dela.

Iskrena hvala vsem domačim za dolgoletno vzpodbudo, podporo in potrpežljivost.

Kazalo

Seznam uporabljenih kratic

AAA – Authentication, Authorization, Accounting
API – Application Programming Interface (Aplikacijski programski vmesnik)
DNS – Domain Name System (Sistem domenskih imen)
DR – Disaster Recovery (Obnovitev po nesreči)
EDS – Elektronski dokumentni sistem
ETZ – Enotne tehnološke zahteve
HKOM – Hitro komunikacijsko omrežje državnih organov
IaaS – Infrastructure as a Service (Infrastruktura kot storitev)
IDS – Intrusion Detection Systems (Sistemi za odkrivanje vdorov)
IEC – International Electrotechnical Commission (Mednarodna komisija za elektrotehniko)
IKT – Informacijsko–Komunikacijska tehnologija
IPS – Intrusion Protection Systems (Sistemi za zaščito pred vdori)
ISMS – Information Security Management System (Informacijski sistem upravljanja varnosti)
ISO – International Organization of Standardization (Medn. organizacija za standardizacijo)
NSPU – Načrtuj Stori Preveri Ukrepaj
PaaS – Platform as a Service (Platforma kot storitev)
RPO – Recovery Point Objective (Točka okrevanja)
RTO – Recovery Time Objective (Čas okrevanja)
SaaS – Software as a Service (Prorgamska oprema kot storitev)
SLA – ServiceLevelAgreement (Sporazum o ravni storitev)
SQL – Structured Query Language (Strukturiran jezik poizvedb)
SUIV – Sistem za Upravljanje Informacijske Varnosti
TSM – Tivoli Storage Manager
URL – Uniform Resource Locator (Naslov spletnega mesta)
UVDAGA – Uredbe o varstvu dokumentarnega in arhivskega gradiva
VPN – Virtual Private Network (Virtualno zasebno omrežje)
ZEKOM – Zakon o elektronskih komunikacijah
ZEPEP – Zakon o elektronskem poslovanju in elektronskem podpisu
ZTP – Zakon o tajnih podatkih
ZVDAGA – Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih
ZVO – Zakon o varstvu okolja
ZVOP–1 – Zakon o varstvu osebnih podatkov

Povzetek

Diplomska naloga govori o vzpostavljanju mnogih varovalnih mehanizmov z namenom zagotavljanja neprekinjenega poslovanja organizacij. Osrednja tema diplomskega dela je bila izdelava varnostnih kopij podatkov, s čimer se poskušajo organizacije izogniti scenariju "po toči zvoniti je prepozno".

Cilj naloge je proučitev možnosti za rešitev problematike varnostnega kopiranja organizacije "Z", ki je zaradi neprestanega večanja količine podatkov in dotrajanih sistemov pred pomembnimi odločitvami.

Tako smo v prvem delu naloge predstavili dejavnosti, ki ogrožajo varnost podatkov ter kako obvladovati tveganja. Seznanili smo se z družino standardov ISO/IEC 27000, ki prispevajo k ustvarjanju varnostne politike organizacije. Predstavili smo načine in in tehnologije, ki se jih organizacije poslužujejo pri zmanjševanju tveganj. Sistem za upravljanje informacijske varnosti olajša zagotavljanje skladnosti z zahtevami veljavne zakonodaje, ki usmerja poslovanje organizacij.

Drugi del naloge je osredotočen na varnostno kopiranje informacij v organizaciji "Z". Po zahtevah standarda ISO/IEC 27001 ima organizacija na področju varnostnega kopiranja informacij vzpostavljenih več kontrol, od delitve na kritične podatke glede izgube in delitve glede kritičnosti za povrnitev delovanja v tveganih situacijah, do dnevnih kontrol nad uspešnostjo izdelave varnostne kopije in kontrol glede iznašanja trakov. Podrobneje smo obdelali ustreznost oblačnih storitev za potrebe organizacije.

V končnem delu diplomske naloge so podane rešitve, ki narekujejo možnost nadaljevanja uporabe sedanje družine diskovnih sistemov, ki omogočajo boljšo strategijo okrevanja po nesreči. Kljub temu organizacija aktivno spremlja razvoj storitev v oblaku in presoja o primernosti prehoda v oblak.

Ključne besede

Standard ISO/IEC 27000, varnostno kopiranje, tveganje, varnostna tehnologija, varnostno kopiranje v oblaku, grožnje.

Abstract

The diploma talks about restoration of several safety mechanisms with the purpose of ensuring continuous operation of organizations. The central theme of the diploma was making backup data files used by organizations to avoid the “it's no use trying to lock the stable door after the horse has bolted” scenario. The aim of the diploma is to research the possibility for salving the problem of backing up by the “Z” organization, which is facing important decisions due to continuous growth of data quantity and worn out systems.

Therefore, we have represented in the first part of the diploma the activities that endanger the safety of data, and how to manage the risks. We became familiar with the family of the ISO/IEC 27000 standards that contribute to creation of the safety policy of an organization. We introduced ways and technologies used by organizations to reduce risks. The information safety management system relieves the assurance of compliance with demands of the current legislation that guides operation of organizations.

The second part of the diploma focuses on backing up of information in the “Z” organization. According to demands of the ISO/IEC 27001 standard, an organization has several controls set up in the field of backing up information - from division into critical data as for their loss, and division as to the criticalness for restoration of operation in risky situations to daily controls over efficiency of making backup copies, and control regarding to physical movement of data tapes. We handled in detail the suitability of cloud for the needs of the organization.

In the final part of the diploma are given solutions that dictate the possibility of continuing the use of the current family of disc systems that enable a better recovery strategy after an accident. Despite that, the organization actively monitors the development of the activities in a cloud and judges the suitability of crossing into a cloud.

Keywords

ISO / IEC 27000, backup, risk, threats, safety technology, the backup in the cloud.

1 Uvod

Za diplomsko nalogo o izdelavi varnostnih kopij pri zagotavljanju nemotenega poslovanja organizacij sem se odločila, ker so raziskave na tem področju zelo velik izziv. Glede na to, da smo v obdobju velike gospodarske krize, odpuščanj, nezadovoljstva, plačilne nedisciplineipd., je moto tistih, ki delujejo nezakonito, vsak dan močnejši. Na drugi strani pa predstavlja informacijska varnost organizacijam, ki si na trgu konkurenčnosti prizadevajo zniževati stroške in povečati donos, zelo trd oreh.

Podjetja oziroma organizacije hranijo velike količine različnih zaupnih informacij o zaposlenih, strankah, proizvodih, raziskavah, finančnem stanju. Večina teh informacij je shranjena na računalnikih in jih lahko prenesemo oziroma do njih dostopamo preko mreže tudi iz drugih računalnikov. Kaj bi se zgodilo s podjetjem, če bi prišlo do daljše prekinitve dostopa do interneta, elektronske pošte in ključnih aplikacij ali izgube določenih podatkov, objave poslovnih skrivnosti na spletu, kraje patentov? Zaupni podatki bi lahko padli v roke konkurenta. Posledice so lahko usodne, od izgube posla do drugih gospodarskih škod, vse do propada podjetja. V najboljšem primeru je zgolj lekcija za prihodnost. Varovanje zaupnih podatkov je tako poslovna pa tudi etična in pravna zahteva.

Tako postaja področje informacijske varnosti v zadnjih letih vse pomembnejše. Organizacije se vedno bolj zavedajo, kako pomembna je zaupnost, celovitost in dostopnost informacij, s katerimi poslujejo. Te informacije želijo ustrezno zaščititi, seveda z namenom ohraniti in razvijati svoje poslovanje še naprej. Zato uvajajo sisteme za upravljanje z informacijsko varnostjo.

V nalogi želimo predstaviti, da je varnost informacijskih sistemov res zelo pomembna. Prikazali bomo celovito informacijsko varnostno politiko, ki pripomore k varovanju ključnih poslovnih procesov in informacij vsake organizacije. Ogledali si bomo, kako poteka vzpostavitev sistema za upravljanje varovanja informacij v organizaciji. V zadnjih letih se informacijska varnost razvija v smeri, ki jo opredeljujejo standardi. Predstavili bomo serijo standardov ISO/IEC 27000, ki pripomorejo tudi k lažjemu zagotavljanju skladnosti z zakonodajo. Še posebej bomo izpostavili varnostno kopiranje informacij, saj analize tveganj, izdelane na osnovi groženj, kažejo na to, da podatki organizacij nikakor niso varni pred izgubo.

V drugem delu pa sledi predstavitev izbrane organizacije in analiza stanja na področju njihovega varnostnega kopiranja podatkov. Zaradi zaupnosti podatkov je ime organizacije in nekaterih internih poimenovanj izmišljeno. Predstavljene so metode in izzivi, ki so prisotni pri zagotavljanju nemotenega poslovanja organizacije in delovanju njihovega informacijskega sistema. Na osnovi pregleda obstoječega stanja, metod, izkušenj in ciljev je na koncu podan predlog za izboljšave, ki bi omogočile preprosto, sistematično ter učinkovito upravljanje in vzdrževanje sistema za varovanje informacij organizacije.

2 Informacijska varnost

2.1 Uvod

Varovanje informacij ni samo tehnološki problem, problem informatike in informatikov, ampak gre pri tem za problem upravljanja. Področje, ki zagotavlja informacijsko varnost, je zato izredno široko in zahteva celovit pristop. Tehnični in organizacijski ukrepi so predpisani z navodili, priporočili, drugimi postopki, standardi in politikami.

Tako bomo v tem poglavju opredelili, kaj predstavlja pojem varnosti v organizacijah na splošno in varnost, kot jo obravnavamo na področju informacijskih sistemov. Predstavili bomo informacijsko varnostno politiko in ker pomemben del pri ustvarjanju varnostne politike prispevajo standardi, bomo predstavili družino standardov ISO/IEC 27000. Osnovo standarda ISO/IEC 27001 predstavlja Sistem za Upravljanje Informacijske Varnosti (SUIV), ki v organizaciji olajša zagotavljanje skladnosti z zahtevami veljavne zakonodaje. Predstavili bomo, kako poteka vpeljava SUIV v organizacijo in opisali nekaj zakonov, ki jim morajo različne organizacije pri svojem poslovanju slediti prav z vpeljavo SUIV. Organizacije morajo biti pri poslovanju še posebej pozorne na grožnje, zato bomo izpostavili dogodke in dejavnosti, ki ogrožajo njihovo poslovanje. Verjetnosti, da se zaradi grožnje, ki izkoristi ranljivost sredstva, povzroči škoda organizaciji, rečemo tveganje. Predstavljamo, katerih načinov se organizacije poslužujejo pri zmanjševanju tveganj in katere tehnologije so jim pri tem v pomoč. Ker je "po toči zvoniti prepozno", je bolj smiselna in stroškovno ugodnejša rešitev kot izguba podatkov izdelava varnostnih kopij vseh pomembnih informacij, kar je osrednja tematika dela.

2.2 Varnost v organizacijah

Varnost organizacije se v prvi fazi začne z zapisanimi pravili, ki določajo, kako morajo zaposleni ravnati v primeru incidentov, hkrati pa paziti, da do njih sploh ne bi prišlo. Ta pravila in varnostna navodila, ki jih organizacija uporablja, so združena v varnostni politiki organizacije.

Dejstvo je, da absolutno varnega sistema ni. Pravzaprav so najšibkejši element varnostnega sistema legalni uporabniki sami. Nadzor le–teh je veliko težje obvladljiv kot pa varovanje tehnoloških virov. Hkrati pa določa stopnjo varnosti tudi osveščenost uporabnikov pri uvajanju varnostnih mehanizmov [1].

V slovenskih korporacijah in organizacijah namenjajo varnosti določeno pozornost prek dokazil o nekaznovanosti, pospravljenih miz, omar z dokumenti, zaklepanja poslovnih prostorov.

Pomen celovitega obvladovanja varnosti dojemajo različne organizacije zelo različno in se zaradi svojih posebnosti vprašanja varnostne kulture v svojih okoljih lotevajo zelo različno. Vendar pa v vsaki veliki organizaciji obstajajo strateški dokumenti, povezani z vsebino krovne varnostne politike. Posebno v organizacijski obliki javne uprave je normativnemu delu varnosti namenjeno razmeroma veliko pozornosti [9].

Organizacijam predstavlja faza izvajanja vseh teh predpisov v praksi velik izziv. Ti predpisi in navodila namreč predstavljajo podlago za izdelavo pravilnikov na nižjih ravneh delovanja. Varnostna kultura pa med zaposlenimi ni prepoznana kot ena izmed pomembnih vrednot [9].

V nadaljevanju se bomo osredotočili zgolj na varnost, ki se navezuje na informacijske sisteme in je tudi zelo obsežno področje. Nanaša se na [3]:

- zaupnost podatkov,
- zaščito informacijskih sistemov proti nepooblaščenim dostopom,
- zagotavljanje razpoložljivosti servisov in podatkov,
- preprečevanje prekinitev in nepooblaščenega prestrezanja podatkov,
- potrjevanje, da so podatki, ki so bili poslani, prejeti ali arhivirani, kompletni in nespremenjeni,
- verodostojnost overitve,
- zaščito proti zlonamernim programom.

Ker je varnost informacijskih sistemov tako obsežno področje, ga je treba zelo skrbno razdelati in načrtovati. Varnost je mogoče razdeliti na dve področji [3]:

- Zanesljivost sistema pomeni zagotavljanje razmer za nemoteno delovanje storitev in normalno delo uporabnikov. To pomeni, da je delovanje informacijskega sistema neprekinjeno in ne odpove vsake toliko časa. Podatki, ki jih uporabnik vnaša v podatkovne zbirke, se ne smejo izgubljati. Rezultati njihove obdelave morajo biti pravilni ipd. Pri tem imata pomembno vlogo organiziranost poslovanja in usposobljenost uporabnikov.

- Zaščita sistema preprečuje izvajanje nelegalnih storitev. To pomeni, da je potrebno informacijski sistem zavarovati tako, da je onemogočeno izvajaje storitev, za katere ta ni predviden. Po drugi strani pa je potrebno skrbeti za preprečevanje dostopa do virov sistema neregularnim uporabnikom – vdiralcem.

2.3 Opredelitev informacijske varnostne politike

Informacijska varnostna politika izraža politiko, s katero želi organizacija zaščititi informacijsko premoženje, ki ga upravlja. Ker je varnostna politika v pristojnosti vodstva, jo vodstvo potrdi in o njej seznani zaposlene. Pomembno je, da je napisana jasno in enostavno ter je razumljiva tudi neveščim uporabnikom [1, 13].

Varnostna politika informacijskega sistema je dokument, ki natančno definira področja varovanja informacijskega sistema, kot so uporaba omrežja, interneta, zasebnost podatkov, ukrepanje ob varnostnih grožnjah, varovanje dokumentov, zaščita virov in ljudi v podjetju.

Ta dokument mora biti prebran in podpisan s strani zaposlenih. Upoštevati ga mora vodstvo, zaposleni, osebe pogodbenih izvajalcev in vsi, ki imajo dostop do premoženja organizacije. Lahko je objavljen na intranetu organizacije, notranjem omrežju, do katerega dostopajo vsi zaposleni, ki imajo vpogled vanj. Določi se skrbnik dokumenta, ki je zadolžen za njegovo vzdrževanje in preglede [13, 21].

Varnostna politika informacijskega sistema je celovit načrt varnosti informacijskega sistema, kjer so zajeta vsa organizacijska pravila, dejavniki in postopki, ki vplivajo na to, da je delovanje celotnega informacijskega sistema varno in zanesljivo [17].

Je množica natančno opredeljenih ciljev, napotkov, pravil in odgovornosti v zvezi z varnostjo informacijskih virov organizacije. Tudi za zaposlene pomenijo ta pravila splošna navodila in naloge za delo, odgovornosti ter način obnašanja. Vsako namerno ali nenamerno dejanje, ki ne upošteva teh pravil, se obravnava kot kršenje.

Varnostna politika ima kar nekaj slabosti, kot so [7]:

- ni dokumentov o varnostni politiki,
- ni načrta ukrepanja v primeru nesreč,
- ni predpisov o dopolnjevanju ali spremembah programske in strojne opreme,
- odsotnost nadziranja varnosti,
- brezbrižnost pri poslovanju.

Kljub temu pa z uvajanjem informacijske varnostne politike organizacija zmanjšuje tveganja na sprejemljivo raven in omogoča uresničevanje naslednjih temeljnih ciljev [13]:

- zavarovanje podatkov pred nepooblaščenim dostopom, obdelavo in razkritjem,
- ohranitev celovitosti informacij in preprečevanje nepooblaščenih sprememb,
- razpoložljivost informacij in virov, ko jih pooblaščeni potrebujejo,
- priprava, vzdrževanje in preverjanje načrtov neprekinjenega poslovanja v obsegu, ki je praktično izvedljiv,
- izobraževanje o informacijski varnosti,
- beleženje in raziskovanje kršitev ter sum teh kršitev,
- preverjanje skladnosti z zakonodajo,
- upoštevanje priporočil glede standardov informacijske varnosti.

2.4 Standardi

Standard je zapisan dogovor, ki vsebuje tehnične specifikacije ali druge natančne zahteve, ki naj bodo stalno uporabljene kot pravila oziroma smernice. Skladnost s standardom za izdelek oziroma storitev pomeni preprečevanje napak, skladnost materialov, proizvodov, procesov in storitev. To pa zagotavlja zanesljivejše delovanje, zmanjševanje posegov zaradi napak in zmanjševanje stroškov [1].

Organizacija, ki ima dobro zasnovano in vpeljano politiko, lahko pridobi tudi certifikat po enem izmed standardov. S tem organizacija poveča svoj ugled in lažje zagotavlja skladnost z zakonodajo, ki se v zadnjih letih v smislu informacijske varnosti razvija v smeri, ki jo opredeljujejo ti standardi.

Na področju varovanja informacij je na voljo več standardov, dobrih praks, postopkov, politik in metodologij. Eden izmed njih je rastoča množica standardov ISO/IEC 27000. To je skupina mednarodnih standardov za upravljanje informacijske varnosti, ki jih je objavila Mednarodna organizacija za standardizacijo (International Organization for Standardization – ISO) skupaj

z Mednarodno elektrotehniško komisijo (International Electrotechnical Commission – IEC). Skupina navedenih standardov predstavlja priporočila za upravljanje informacijske varnosti ter tveganj [8, 17, 21].

Družino standardov 27000 sestavljajo [8]:

- ISO/IEC 27000: Slovar in definicije,
- ISO/IEC 27001: Specifikacije sistema za upravljanje informacijske varnosti (SUIV),
- ISO/IEC 27002: Primeri dobre prakse implementacije sistema za upravljanje informacijske varnosti (SUIV),
- ISO/IEC 27003: Napotki za načrtovanje in vpeljavo sistema za upravljanje varovanja informacij (SUIV),
- ISO/IEC 27004: Merila za ocenjevanje učinkovitosti sistema za upravljanje varovanja informacij (SUIV),
- ISO/IEC 27005: Upravljanje varnostnih tveganj,
- ISO/IEC 27006: Smernice za organe, ki presojajo in certificirajo sisteme upravljanja informacijske varnosti (SUIV),
- ISO/IEC 27007: Smernice za revidiranje SUIV,
- ISO/IEC 27008, 27010, 27011...

2.4.1 ISO/IEC 27000

Varovanje informacij je povezano s kompleksno terminologijo. Neustrezno definirani pojmi lahko privedejo do zmede in razvrednotenja formalnih ocen in certifikacije. Zato je njegova vsebina zelo pomembna, ker predstavlja splošno sprejet besednjak strokovnjakov s področja varovanja informacij [17].

2.4.2 ISO/IEC 27001

Vsebina standarda je sestavljena iz navodil in aktivnosti, ki so potrebne za načrtovanje, vzpostavitev, izvajanje in vzdrževanje sistema za upravljanje informacijske varnosti (SUIV) ter izboljševanje SUIV na osnovi sprememb in novih zahtev. Verzija 2005 podaja model za strukturiranje procesov NSPU (načrtuj–stori–preveri–ukrepaj). Zadnja različica 2013 pa daje večji poudarek zahtevam za ocenjevanje in identifikacijo informacijskih varnostnih tveganj.

2.4.3 ISO/IEC 27002

Standard podaja priporočila najboljše prakse za upravljanje varovanja informacij in smernice za certificiranje v skladu z ISO/IEC 27001. Standard je vodnik in v pomoč pri vodenju projekta s ciljem doseganja skladnosti s standardom ISO/IEC 27001. Pri različici 2013 so bile nekatere kontrole odstranjene, nekatere preoblikovane ter dodane nove kontrole, ki obravnavajo razvoj na področju tehnologij (računalništvo v oblaku).

2.4.4 ISO/IEC 27003

Standard ISO/IEC 27003:2010 daje jasna navodila o načrtovanju projekta SUIV v organizacijah in smernice o pridobivanju privolitve uprave za izvedbene načrte. Torej, uporaba teh smernic zagotavlja organizaciji okvir za učinkovito informacijsko varnost in zaupanje, s tem ko obvladuje tveganja.

2.4.5 ISO/IEC 27004

Namen standarda je pomagati organizacijam ukrepati, poročati in s tem sistematično izboljšati učinkovitost njihovega varnostnega sistema za upravljanje informacij (SUIV). Standard zajema smernice za opredelitev in uporabo merilnih tehnik za zagotavljanje zanesljivosti.

2.4.6 ISO/IEC 27005

Ta standard opisuje proces upravljanja tveganj na področju informacijske varnosti. Podpira splošne pojme, opredeljene v standardu ISO/IEC 27001, in je zasnovan tako, da daje priporočila pri zadovoljivem izvajanju informacijske varnosti, ki temelji na upravljanju s tveganji. Ne določa in ne predlaga nobene posebne metode glede analize in ocenjevanja tveganj, ampak mora organizacija sama prepoznati metodologijo, ki najbolj ustreza njenemu SUIV in zakonskim zahtevam [8].

2.4.7 ISO/IEC 27006

Standard določa formalne pogoje za certifikacijo organizacij skladno s standardom ISO/IEC 27001. Zagotavlja, da so certifikati ISO/IEC 27001, ki so izdani organizaciji, smiselni in vredni zaupanja, torej zanesljivi [8].

2.4.8 ISO/IEC 27007

Standard daje napotke sistemu za upravljanje informacijske varnosti (SUIV) o reviziji programa, izvedbi revizije ter o pristojnosti notranjih in zunanjih revizorjev.

2.5 Sistem za upravljanje informacijske varnosti – SUIV

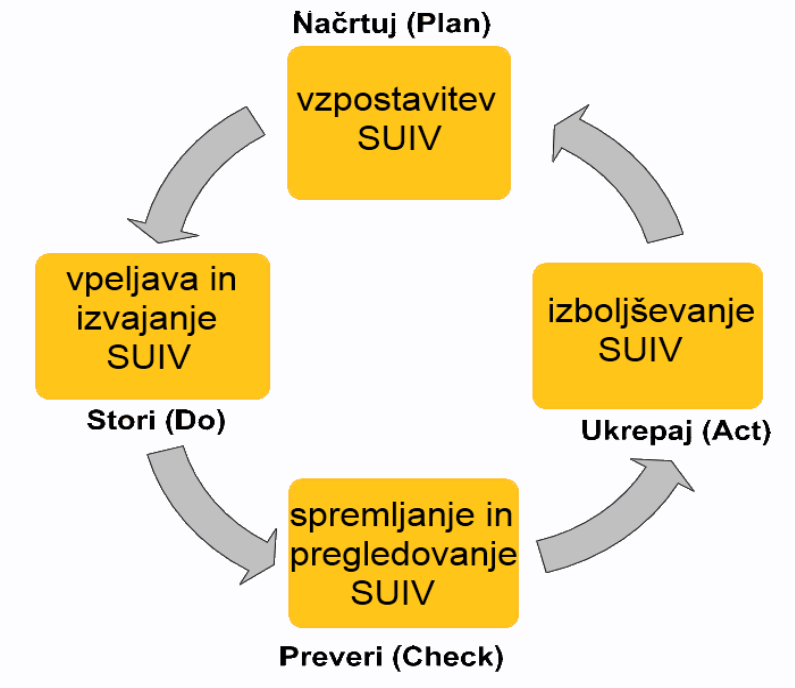
V organizacijah skrbi za vzpostavitev, vpeljavo, vzdrževanje in nenehno izboljševanje na področju informacijske varnosti sistem za upravljanje informacijskega varovanja (v nadaljevanju SUIV) ali ang. ISMS (Information Security Management System). Je osnova standarda ISO/IEC 27001. Temelji na ciljih, ki jih organizacija želi doseči z varovanjem in zaščito, na izbiri ustrezne strategije, ki mora ustrezati velikosti podjetja, načinu in obsegu poslovanja, virih, organizacijski kulturi ter znanju [2].

Uvedba sistema SUIV za organizacijo pomeni marsikatero pridobitev [11]:

- večja zanesljivost storitev, s tem ko se izboljšuje nivo varnosti informacij,

- večja kakovost poslovnih procesov in povečanje razpoložljivosti storitev,
- ugled in boljše mesto na trgu konkurence, s tem ko izpolnjuje pogoje za certifikacijo po standardu ISO/IEC 27001,
- skladnost z zakonodajo,
- znižanje tveganja nepooblaščenega dostopa do informacij.

Tako kot vsi ostali upravljavski sistemi tudi SUIV za vzpostavitev in upravljanje uporablja procesni pristop NSPU (načrtuj–stori–preveri–ukrepaj), kot prikazuje Slika 1.



Slika 1: Procesni pristop SUIV

2.5.1 Načrtuj (vzpostavitev SUIV)

Ključni del prve faze vzpostavitve SUIV je izdelava načrta vzpostavitve. Ta načrt mora sprejeti in potrditi najvišje vodstvo organizacije, ki mora zagotoviti tudi dovolj sredstev za realizacijo. Osnova vzpostavitve okvira SUIV pa je izdelava analize in ocene tveganj, kar je zelo pomemben, zahteven in obsežen del celotnega projekta. Potrebno je obdelati veliko množico podatkov s pomočjo raznih programskih orodij. Za ključne procese je potrebno ugotoviti časovni okvir, v katerem mora biti po uresničitvi grožnje varnosti informacijska podpora ponovno vzpostavljena [26, 27].

2.5.2 Stori (vpeljava in izvajanje SUIV)

Ko vodstvo sprejme in potrdi dokument o politiki varovanja podatkov, ki vključuje oceno tveganja, lahko organizacija prične z izvedbo celotnega projekta vzpostavitve SUIV. Najprej je potrebno izdelati načrt izvedbe na več nivojih, do najnižjega nivoja, ki zagotavlja operativno izvajanje vseh potrebnih aktivnosti za doseganje želenega nivoja informacijske

varnosti. Z vsemi aktivnostmi uvajanja SUIV morajo biti seznanjeni vsi zaposleni in zunanji sodelavci ter pogodbeni partnerji organizacije.

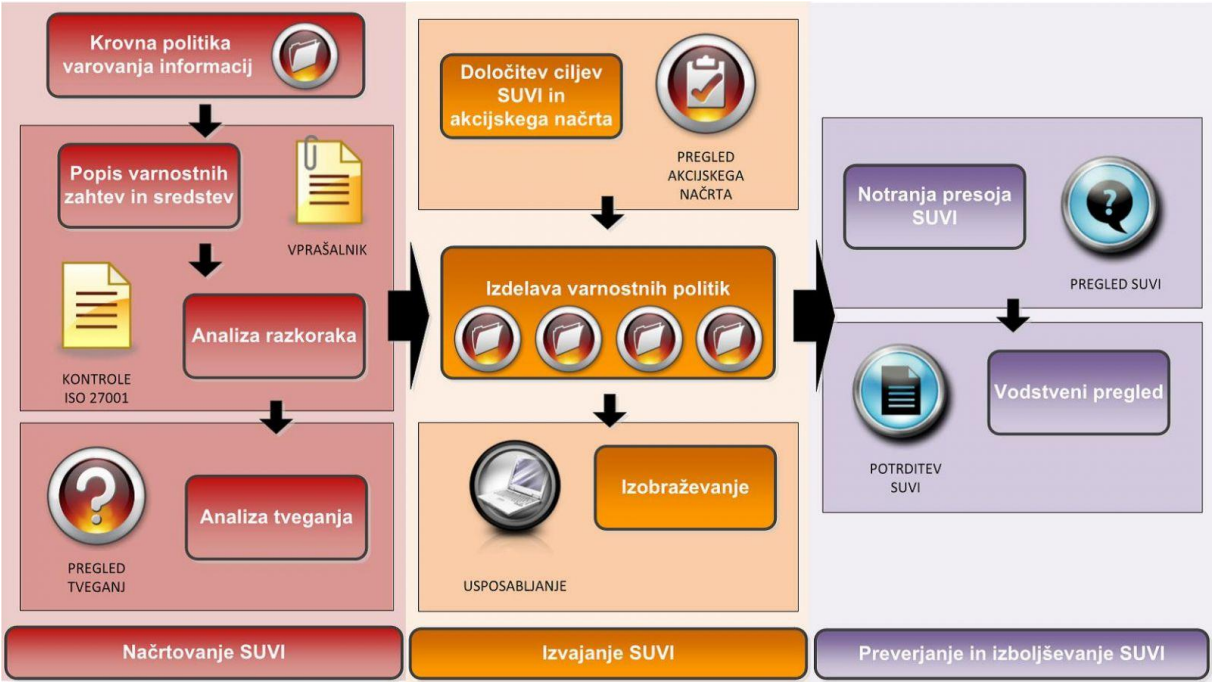
2.5.3 Preveri (spremljanje ter pregledovanje SUIV)

V tej fazi gre za vzpostavitev sistema kontrol nad delovanjem SUIV, saj mora vodstvo organizacije ves čas skrbno spremljati, ali se aktivnosti v okviru SUIV odvijajo po pričakovanjih. Določijo se odgovorne osebe za izvajanje teh kontrol, hkrati pa mora biti poskrbljeno za informiranje in usposabljanje vseh zaposlenih s temi kontrolami. Rezultate učinkovitosti delovanja SUIV je potrebno redno presojati, obravnavati povratne informacije vseh uporabnikov ter beležiti aktivnosti, ki lahko kakorkoli vplivajo na učinkovitost SUIV.

2.5.4 Ukrepaj (vzdrževanje ter izboljševanje SUIV)

Četrta faza vzpostavitve SUIV v organizaciji je analiza odstopanj in izvajanje preventivnih ukrepov. Poteka vzdrževanje aktivnosti na ustrezni ravni oziroma se uvajajo izboljšave, če analize odstopanj pokažejo, da je potrebno določila v posameznih dokumentih SUIV spremeniti. Potrebno je zagotoviti dodatno usposabljanje ali ustreznejši način informiranja zainteresiranih strank.

Celotni model vzpostavitve SUIV z vsemi fazami vzpostavitve in glavnimi aktivnostmi znotraj posamezne faze prikazuje Slika 2.



Slika 2: Faze SUIV procesa po standardu ISO/IEC 27001

Seveda pa proces SUIV postavlja organizacijo pred mnoge izzive, od tega, da je potrebno zbrati veliko količino podatkov, s pomočjo katerih se izdela analiza tveganja. Predvsem pa je vodstvo tisto, ki mora razpoznati dodano vrednost k poslovanju organizacije.

2.6 Skladnost z zakonodajo

Vpeljava SUIV v organizacijo olajša zagotavljanje skladnosti z zahtevami veljavne zakonodaje, kot so npr.:

- Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA),
- Uredba o varstvu dokumentarnega in arhivskega gradiva (UVDAGA),
- Enotne tehnološke zahteve (ETZ),
- Zakon o varstvu osebnih podatkov (ZVOP−1),
- Zakon o tajnih podatkih (ZTP),
- Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP),
- Zakon o elektronskih komunikacijah (ZEKOM),
- Zakon o varstvu okolja (ZVO).

ZVDAGA določa pogoje za zajem in pretvorbo gradiva v digitalno obliko, hrambo tega gradiva v fizični in elektronski obliki, veljavnost oziroma dokazno vrednost takega gradiva, varstvo arhivskega gradiva in pogoje za njegovo uporabo, naloge arhivov in javne arhivske službe ter s tem povezane storitve in nadzor nad izvajanjem [29].

UVDAGA ureja delovanje in notranja pravila organizacij, ki hranijo dokumentarno oziroma arhivsko gradivo, hrambo tega gradiva v fizični in digitalni obliki, splošne pogoje, registracijo in akreditacijo opreme in storitev za digitalno hrambo, odbiranje in izročanje arhivskega gradiva javnim arhivom, strokovno obdelavo in vodenje evidenc arhivskega gradiva, varstvo arhivskega gradiva, uporabo arhivskega gradiva v arhivih ter delo arhivske komisije [22].

ETZ podrobneje opredeljujejo poslovne, organizacijske in tehnološke pogoje za izpolnjevanje ZVDAGA, ki ureja področje dolgoročne elektronske hrambe, in na njegovi podlagi izdanih podzakonskih predpisov. ETZ so povezovalni element med zahtevami zakona in potrebami, ki so se izkazale v praksi [6].

ZVOP–1 določa pravice, obveznosti, načela in ukrepe, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika pri obdelavi osebnih podatkov. Obdelava pa pomeni kakršno koli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklicanje, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje; obdelava je lahko ročna ali avtomatizirana (sredstva obdelave) [12].

ZEPEP ureja elektronsko poslovanje, ki zajema poslovanje v elektronski obliki z uporabo informacijske in komunikacijske tehnologije in uporabo elektronskega podpisa v pravnem prometu, kar vključuje tudi elektronsko poslovanje v sodnih, upravnih in drugih podobnih postopkih. S tem zakonom se uvaja enakovrednost elektronskega in lastnoročnega podpisa na dokumentih, kadar so izpolnjeni nekateri pogoji [28].

2.7 Grožnje

Organizacije morajo biti pri oblikovanju varnostne politike pozorne na grožnje, ki izhajajo iz okolja in podjetja samega. Grožnja varnosti informacijskega sistema in s tem grožnja zagotavljanju nemotenega poslovanja organizacije je neželen dogodek ali dejavnost, ki privede do izgube celovitosti, zaupnosti ali razpoložljivosti informacij in onemogoča zadovoljivo delovanje informacijskega sistema [19].

Grožnje izkoriščajo ranljivosti informacijskega sistema, katerih posledica je nastala škoda. Ta se razteza od majhnih posledic, kot je na primer izguba kakega manj pomembnega dokumenta, izguba dobička ali ugleda, pa vse do katastrofalnih posledic, kot bi lahko bilo uničenje informacijskega sistema [1].

Izbira prave strategije pa ni odvisna samo od predvidenih posledic, temveč predvsem od finančnih, kadrovskih, razvojnih in drugih zmožnosti organizacije. Kontrola zato ni samo kurativna, ampak predvsem preventivna.

Grožnje lahko delimo glede na več različnih kriterijev. Pogosta pa je delitev na naslednje tri skupine: izredni dogodki, naključni dogodki in človekova namerna dejavnost. Škodo, ki jo lahko te grožnje povzročijo bomo omejili na področje informacijskih sistemov.

2.7.1 Izredni dogodki

Kot izredne dogodke opredelimo tisto dogajanje, ki ga vnaprej ne moremo napovedati. To so poplave, požari, potresi, strele, izpadi električne energije. Verjetnost, da do takšnega dogodka pride, je relativno majhna, lahko pa pride do poškodb velikih razsežnosti, prekinitve procesa dela ali celo uničenja informacijskega sistema.

- **Požar** lahko neko organizacijo popolnoma uniči in ogroža celotni informacijski sistem. Vzrok za požar je lahko namerno dejanje ali pa je posledica nenamerne dejavnosti človeka. Za preprečitev požara je potrebno upoštevati predpisane varovalne ukrepe [19].

- **Poplava** lahko ogroža informacijske vire, ki niso dvignjeni od tal. Običajno je kriva počena vodovodna cev ali slabe cevi centralne kurjave. Še posebej je to nevarno v nočnem času, ko nihče ne more pravočasno ukrepati. Voda ali druge tekočine lahko na strojni (računalniki, strežniki) in programski opremi (informacijski sistem, podatki) naredijo ogromno škode zaradi nerazpoložljivosti sistema, uničenja ali poškodb [1].

- **Izpad električne energije** lahko povzroči škodo zaradi nedostopnosti sistema in izgube podatkov.

2.7.2 Naključni dogodki

Naključni dogodki, ki predstavljajo nevarnost informacijskemu sistemu, so razne odpovedi, ki so lahko delne ali popolne oziroma postopne ali nenadne [19].

- **Odpoved strojne opreme** je posledica staranja materialov, napačna raba, nepravilno vzdrževanje, nezdružljivost opreme, pregretja, tresljaji, vlaga, udarci in izdelava komponent iz slabših materialov. Vse to lahko povzroči izgubo ali popačenje podatkov in informacij ter delno ali popolno nerazpoložljivost sistema.

- **Programska oprema** lahko vsebuje skrite napake, ki porušijo delovanje sistema in lahko privedejo do izgube podatkov ter nerazpoložljivosti programske opreme [19].

- **Odpoved človeka** je posledica neusposobljenosti, neizkušenosti ali psihičnih in fizičnih preobremenitev. To je lahko vzrok vnosa napačnih podatkov, napačne obdelave informacij, napačnih statistik, odpovedi sistema [1].

2.7.3 Človekova dejavnost

Človekova namerna dejavnost je ena izmed pogosto prisotnih groženj, ki lahko povzroči škodo organizaciji. Pravzaprav je varnost najbolj ogrožena ravno s strani zaposlenih, saj le–ti najbolje vedo, katere podatke iskati in kje. Vzroki so zelo različni, od osebne koristi, kot je želja po dokazovanju, do povzročitve škode zaradi prekinitve delovnega razmerja.

- **Kraja** iz podatkovnih zbirk pomeni, da si nepooblaščena oseba pridobi določene ključne občutljive podatke in informacije ter organizaciji povzroči škodo. Materialno škodo lahko povzroči tudi kraja opreme, zato je kraja resna varnostna grožnja vsem sredstvom podjetja [1].

- **O nepooblaščenem dostopu** do sistema govorimo takrat, ko napadalec ali vsiljivec skuša priti do podatkov, virov in storitev v sistemu. Napadalci so lahko zunanji ali notranji in zelo različno spretni. Vse pogostejši in nevarni so napadi z resnimi posledicami za računalniške sisteme, saj za vdor v računalniški sistem običajno ni potrebno veliko znanja in vloženega truda. Kaže se celo, da je računalniška kriminaliteta zelo donosen posel, saj niso potrebne velike investicije, pridobljena korist je lahko zelo velika, hkrati pa obstaja majhna možnost za identifikacijo napadalca.

- **Trojanski konji** so programi, ki sicer izvajajo uporabne procese, vendar so to za uporabnika neželene in neznane operacije, najpogosteje zlonamerne aktivnosti. Trojanski konji se samodejno ne razmnožujejo. Posebni primer trojanskega konja je vohunska programska oprema, ki zbira gesla, ko jih tipkamo na tipkovnici, informacije o obiskovanih spletnih straneh, poleg tega beleži, kateri programi se nahajajo na računalniku in katere informacije pošilja uporabnik po internetu [7].

- **Računalniški virus** je programska koda, ki se širi in prenaša brez vednosti in volje uporabnika. S tem ko uporabnik okuženo datoteko odpre, se računalniški virus razširi in okuži izvršne programske datoteke. Ko se razmnoži, lahko virus prične s škodljivim delovanjem, kot je lahko tudi izbris podatkov [7].

- **Računalniški črv** (worm) je prav tako kot virus zlonamerna koda, ki pa za svoje delovanje ne potrebujejo uporabnikovega programa. Za širjenje ne potrebujejo ročne pomoči, ampak izkoriščajo obstoječe povezave med računalniki. Črvi se lahko hitro

razmnožujejo in na tak način porabljajo sredstva ter upočasnijo delovanje računalnikov in omrežij ali povzročijo celo popolno sesutje omrežja [1].

- **Vohun** (spyware) je tista programska oprema, ki je običajno pripeta kot skrita komponenta preizkusnim (shareware) ali brezplačnim (freeware) aplikacijam, ki jih prenesemo preko spleta. Lahko pa se neželeni program tudi samodejno namesti ob obisku spletne vsebine. Ko je vohun enkrat nameščen, spremlja internetne aktivnosti uporabnika in nato sporoča te informacije napadalcu. Najhujša oblika vohunov so opazovalci tipkovnice, ki si zapisujejo tipke, ki jih pritiskamo, in tako pridejo do številk kreditnih kartic in uporabniških gesel [19].

- **Spletni piškotki** (cookies) so majhne besedilne datoteke, ki jih na disku uporabnikovega računalnika ustvarijo obiskane spletne strani. Gre za vohljanje skrbnika obiskanega spletišča, ko si le–ta pridobi marsikatero uporabnikovo informacijo. Z njihovo pomočjo si lahko spletne strani zapomnijo uporabnikovo personalizirano vsebino.

- **Nadležna pošta** (spam) je pošiljanje enakih ali podobnih sporočil na veliko število naslovov. S takšnimi sporočili oglaševalci, ki naslove prejemnikov pridobivajo s forumov, spletnih strani, podatkovnih baz ali ugibanjem, oglašujejo razne izdelke in storitve.

- S**pletno ribarjenje** (phishing) je nezakonito pridobivanje uporabnikovih osebnih podatkov. Prevarant s pomočjo lažnih spletnih strani in elektronskih sporočil poskuša uporabnike prepričati, da vanjo vnese finančne podatke ali razna gesla [16].

- **Napad na gostiteljevo datoteko** (pharming) predstavlja neposreden napad na strežnike DNS ali datoteko (host file) na uporabnikovem računalniku. Prevarant prepiše host datoteko z lažnimi naslovi. Ko uporabnik vnese pravilen URL naslov, je preusmerjen na lažno stran, ki jo je ustvaril napadalec. Tako skuša prevarant od uporabnika izvabiti podatke, ki bi jih lahko kasneje uporabil na originalni strani.

- **Socialni inženiring** izkorišča omrežja za spletno druženje. Napadalec skuša s pomočjo različnih tehnik prepričati uporabnika sistema v to, da mu izda avtentikacijske podatke, s katerimi se lahko nezakonito prijavi v sistem [16].

2.8 Tveganja

Posledica zgoraj naštetih groženj je tveganje, kateremu je izpostavljena vsaka organizacija. Pravzaprav je tveganje prisotno povsod, tako na delovnem mestu, kot tudi pri drugih opravilih. Če torej poznamo grožnje, lahko ustrezno obravnavamo tveganja in zagotovimo varnejše delo organizacije same ter višji nivo varnosti informacijskega sistema.

Tveganje je negotovost nastanka dogodka, ki lahko negativno vpliva na doseganje strateških, operativnih in finančnih ciljev organizacije. Vodstvo mora opredeliti tveganja, ki ogrožajo poslovanje organizacije in jih z ukrepanjem obvladovati na sprejemljivi ravni [20].

Tveganje je verjetnost, da zaradi nekaterih trenutnih procesov ali dogodkov, ki jih imenujemo grožnje, nastane škoda v organizaciji. Informacijsko tveganje je tako verjetnost škode na področju informacijske izgube oziroma okvare pri zaupnosti, celovitosti oziroma razpoložljivosti informacijskega sistema [14].

Zato dobra varnostna politika predvideva tudi izdelavo analize tveganj. Analiza tveganj je postopek, s katerim je formalno predstavljen proces ocene verjetnosti nastanka tveganj in njihovih posledic ter ukrepov, ki so potrebni za zagotavljanje doseganja ciljev. Analiza tveganj ni enkratno dejanje, temveč proces, ki ga je potrebno po vzpostavitvi stalno izvajati in dopolnjevati [20].

Na tak način opredelimo možne kritične točke in odgovorimo na mnoga vprašanja in dileme, kot so:

- Kakšnim grožnjam so izpostavljeni informacijski viri?
- Katere so ranljivosti informacijskih sredstev?
- Kakšno škodo povzroči grožnja preko ranljivosti?
- Kakšno je sprejemljivo tveganje?
- Kaj moramo varovati?

Analiza tveganj je sestavljena iz več faz, v katerih določimo, kaj lahko povzroči potencialno izgubo ter kako, kje in zakaj lahko ta izguba nastane [14]:

- identifikacija sredstev organizacije in ocenitve njene vrednosti,
- prepoznavanje groženj,
- prepoznavanje ranljivosti in verjetnost, da bo le–ta izkoriščena,
- izračun vpliva, ki bi ga povzročena grožnja imela na dobiček,
- identifikacije, izbire in izvršitve primerne kontrole,
- ocenitve produktivnosti merjenja kontrole.

Standard ISO 27005:2008 definira 4 načine soočenja s tveganji [20]:

- izogibanje: organizacija ne opravlja aktivnosti, ki povzročajo to tveganje;
- prenos tveganja na drugo entiteto: na ta način organizacija kompenzira finančne posledice uresničenega tveganja, medtem ko je odgovornost še vedno na strani organizacije;
- blaženje: zmanjšanje škode v primeru, da napadalec uspešno izkoristi ranljivost;
- odobritev oziroma sprejem tveganja: organizacija se odloči, da je tveganje tako, da ga sprejema in ne bo uvedla nobenega od prvih treh načinov.

Vseh tveganj seveda ni možno identificirati, jih izločiti in popolnoma odpraviti. Na osnovi pridobljenih rezultatov ocene tveganja pa lahko organizacija sprejme varnostne ukrepe za izboljšanje varovanja informacij in tako zmanjša njihovo verjetnost. Investicije v sredstva torej načrtuje na tistih področjih, ki so povezana z visokim tveganjem. Nastala škoda se navadno meri v denarju, nematerializirana posledica pa je tudi padec ugleda organizacije.

2.9 Varnostne kopije podatkov

Zaradi številnih možnosti, ki ogrožajo podatke, le–ti na trdih diskih računalnikov nikakor niso varni pred izgubo. Zato v mnogih organizacijah analiza tveganj pokaže, da je izdelava varnostnih kopij vseh pomembnih podatkov najbolj smiselna rešitev in tudi stroški so v primerjavi z izgubo podatkov, za katere organizacija ocenjuje, da so neprecenljivo pomembni, majhni.

Namen varnostnih kopij je torej obnova izgubljenih podatkov oziroma čim prej vzpostaviti delovanje organizacije po izpadu. Izdelane morajo biti sprotno in vestno, saj to ne vzame veliko časa in lahko večino dela opravljajo namenski programi. Vsebino kopij pa je potrebno redno preverjati.

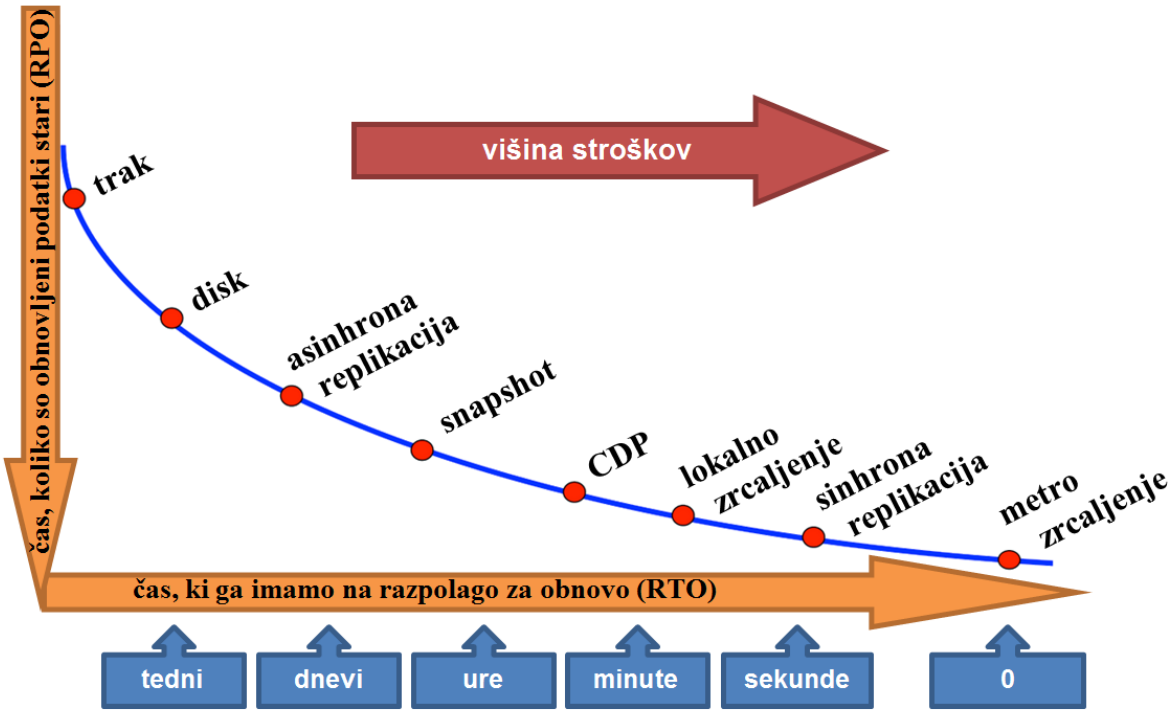
Pojem varnostnega kopiranja se velikokrat istoveti z dolgoročno elektronsko hrambo oziroma dokumentiranjem in arhiviranjem gradiva. Zato je potrebno poudariti, da gre za dva povsem različna pojma. Arhiv je primarno skladišče podatkov, po katerih se sprehajamo vsakokrat, ko želimo do nekega starejšega podatka, varnostne kopije pa uporabimo le ob izgubi podatkov in predstavljajo sekundarni vir.

Predenj pa organizacija začne načrtovati primerne rešitve varnostnega kopiranja, mora znati pravilno ovrednotiti svoje podatke. Seveda morajo biti vsi podatki zaščiteni, le da imajo prednost najbolj kritični podatki. To so tisti podatki, ki se za poslovanje ne smejo izgubiti ali priti do izpada. Nato sledijo pomembni podatki za vsakodnevno delo in še splošni in sprotni dokumenti in datoteke.

Pomemben faktor pri shranjevanju varnostnih kopij je lokacija varnostne kopije. Kopije se nikakor ne shranjuje v istem prostoru, kot je original. V primeru katastrofalnih dogodkov, kot so poplave, požar, kraja, se lahko uniči tako original kot kopija. Zato je priporočljivo varnostne kopije hraniti ločeno. Pomembno je tudi, da hranimo poleg zadnje še starejše kopije, saj se morda lahko zgodi, da izgubljeni podatek najdemo samo na več tednov stari kopiji [23].

Načinov oziroma tehnik za izdelavo varnostnih kopij je več, od traku, diska, replikacije, zrcaljenja, do oblaka, kot prikazuje Slika 3. Za organizacijo pa je odločitev o izbiri odvisna od mnogih dejavnikov [4]:

- najugodnejše razmerje med časom, ki ga imamo na razpolago za obnovo ter koliko stari so lahko obnovljeni podatki;
- količina podatkov, ki mora biti prenešena med dvema lokacijama;
- finančna ocena implementacije ter operativni stroški;
- fleksibilnost aplikacij in protokolov;
- zanesljivost delovanja;
- reference.



Slika 3: Podporne storitve za okrevanje po nesreči

2.9.1 Zapisovanje na medije DVD

Ta način izdelave varnostnih kopij je relativno poceni. Tudi shranjevanje medijev je dokaj enostavno, ker ne zavzamejo veliko prostora. Zaradi majhne kapacitete, je majhna tudi količina podatkov, ki jih lahko spravimo na en medij. V organizacijah z velikimi arhivi bi se jih tako nabralo ogromno. Negotova je tudi njihova življenjska doba, okoli 5 do 10 let, v idealnih pogojih mogoče malo več. Podobna tehnologija so mediji Blu-Ray, ki imajo večjo kapaciteto (25 GB in dvoslojni 50 GB), vendar še vedno iste omejitve kot pri DVD-ju [23].

2.9.2 Shranjevanje na zunanji trdi disk

Prednost zunanjih diskov je enostavnost uporabe in velika kapaciteta. Edina slabost je le dovzetnost za mehanske okvare. Da je kopiranje podatkov in ažuriranje kopije čimbolj enostavno, so na voljo različni programi, ki opravljajo kopiranje namesto nas. Potrebno pa je vestno preverjanje, da je na zunanjem trdem disku popolna varnostna kopija bistvenih podatkov iz računalnika. Dokaj enostavna je v primeru nezgode tudi obnova podatkov iz take kopije [23].

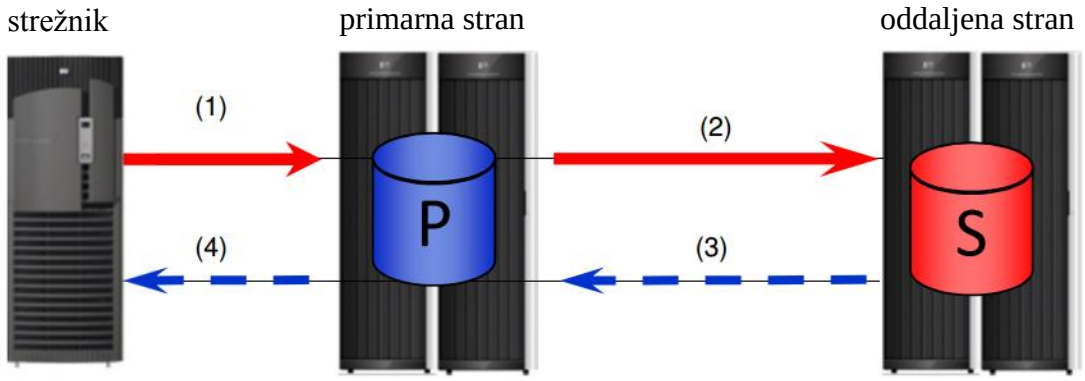
2.9.3 Replikacija

O replikaciji govorimo, kadar ima isti podatek v sistemu lahko več fizičnih kopij, ki so na različnih lokacijah. Replikacija vzdržuje dislocirano ažurno kopijo podatkov ali datotečnega sistema. Za replikacijo baz je predpogoj dovolj hitra povezava med dvema različnima lokacijama in popolnoma identična strojna in programska oprema.

Replikacija je proces, v katerem se ob vsaki spremembi vrednosti podatka, katera koli kopija istega podatka ažurira na novo vrednost. Vendar je lahko to časovno zelo zahtevno, saj se morajo lokacije med seboj najprej dogovoriti o ažuriranju. Sistemu se tako poveča nevarnost nekosistentnosti.

Poznamo dve vrsti replikacij, katerih delovanje prikazuje Slika 4 [5]:

- **Sinhrona replikacija**: strežnik zapiše I/O zahtevo na primarno diskovno polje (1) in čaka na dovoljenje, da se ta zapis se prezrcali na sekundarno diskovno polje (2), sekundarno diskovno polje pošlje potrdilo o sprejemu zapisa (3), strežnik dobi potrdilo o uspešnem zapisu (4) in lahko nadaljuje z zapisovanjem;
- **Asinhrona replikacija**: strežnik zapiše I/O zahtevo na primarno diskovno polje (1), strežnik dobi potrdilo o uspešnem zapisu od primarnega diskovnega polja (4) in lahko nadaljuje z zapisovanjem; korak (2) in korak (3) se za vsak zapis procesirata brez vpliva na strežnik.



Slika 4: Delovanje sinhrone in asinhrone replikacije

2.9.4 Zrcaljenje (mirroring)

O zrcaljenju podatkov govorimo, kadar se s pomočjo krmilnika zapisi neprestano podvajajo na dva fizično ločena diska v realnem času. Na zrcaljenem disku imamo popolno kopijo primarnega diska. V primeru okvare enega izmed diskov, se lahko podatke prebere iz delujočega diska brez kakšnih posebnih tehnologij.

Dobra lastnost zrcaljenja je visoka zanesljivost sistema, slaba pa cena, saj potrebujemo dvakratno velikost diskov za shranjevanje podatkov in še programsko in strojno opremo za obnovitev diska.

Poznamo več načinov zrcaljenja podatkov med dvema oddaljenima podatkovnima centroma za primer obnove po katastrofi :

- **Sinhrono zrcaljenje** (Metro Mirror): za krajše razdalje med lokacijama, I/O operacija je zaključena, ko je podatek shranjen na obeh lokacijah.
- **Asinhrono zrcaljenje** (Global Mirror): za večje razdalje med lokacijama, I/O operacija je zaključena, ko je podatek shranjen na primarni lokaciji.

2.9.5 Shranjevanje v oblak

Z besedo "oblak" poimenujemo računalniške spletne storitve, ki gostujejo zunaj meja neke organizacije. Računalništvo v oblaku pomeni, da so določeni viri strojne in programske opreme na različnih lokacijah, zunaj lokacije uporabnika. To predstavlja alternativo današnji klasični izdelavi varnostnih kopij podatkov. Pojavlja se tudi čedalje več ponudnikov, ki omogočajo izdelavo varnostnih kopij podatkov v oblakih [25].

Varnostno kopiranje te vrste ne zahteva nobene dodatne strojne opreme. Potrebna je le dovolj hitra povezava z internetom. Uporabniki pa glede na dejansko porabo najemajo in tudi plačajo potrebne informacijske vire. Uporabniku tudi ni potrebno skrbeti za nakup, vzdrževanje strojne in programske opreme, ker za to poskrbijo ponudniki.

Sistem za izdelavo varnostnih kopij v oblaku temelji na aplikaciji, ki se nahaja pri uporabniku storitve in se proži v rednih intervalih (urno, dnevno, tedensko itd.). Intervali se opredelijo s pogodbo o uporabi oblačne storitve (SLA – ServiceLevelAgreement) za izdelavo varnostne kopije podatkov. Ker se podatki prenašajo po svetovnem spletu in je podatkovna prepustnost po navadi relativno zelo omejena, se za prenos lahko uporabi pristop inkrementalne izdelave varnostne kopije. To pomeni, da se za zmanjševanje uporabljene pasovne širine pri prenosu podatkov v oblak, prenašajo samo spremembe, ki se zgodijo v primarni podatkovni bazi [24].

Značilnosti oblačnega računalništva [25]:

- uporabnik plača toliko računalniških zmogljivosti, kolikor jih glede na trenutne potrebe rabi;
- obseg zakupljenih shranjevalnih potreb se lahko hitro poveča ali zmanjša, saj oblak nudi neomejene zmogljivosti;
- računalniške zmogljivosti so enostavno dostopne preko standardiziranih mehanizmov;
- centralizirana infrastruktura omogoča enostavnejše posodabljanje programske opreme;
- obstaja veliko ponudnikov oblačnih storitev, ki omogočajo uporabnikom raznolike možnosti;
- računalništvo v oblaku razen klasične virtualizacije uporablja tudi zmožnosti avtomatizacije in združevanja storitev ter sobivanja uporabnikov na istih informacijskih virih;
- oblačni sistemi avtomatično nadzirajo in optimizirajo vire glede na vrsto storitve (npr. hramba, procesiranje, pasovna širina, število aktivnih uporabnikov); transparentnost porabe virov je zagotovljena z njihovim nadzorom in spremljanjem;
- prenos podatkov v oblak oziroma iz njega je omejen s pasovno širino spleta, ki onemogoča hiter prenos velike količine podatkov.

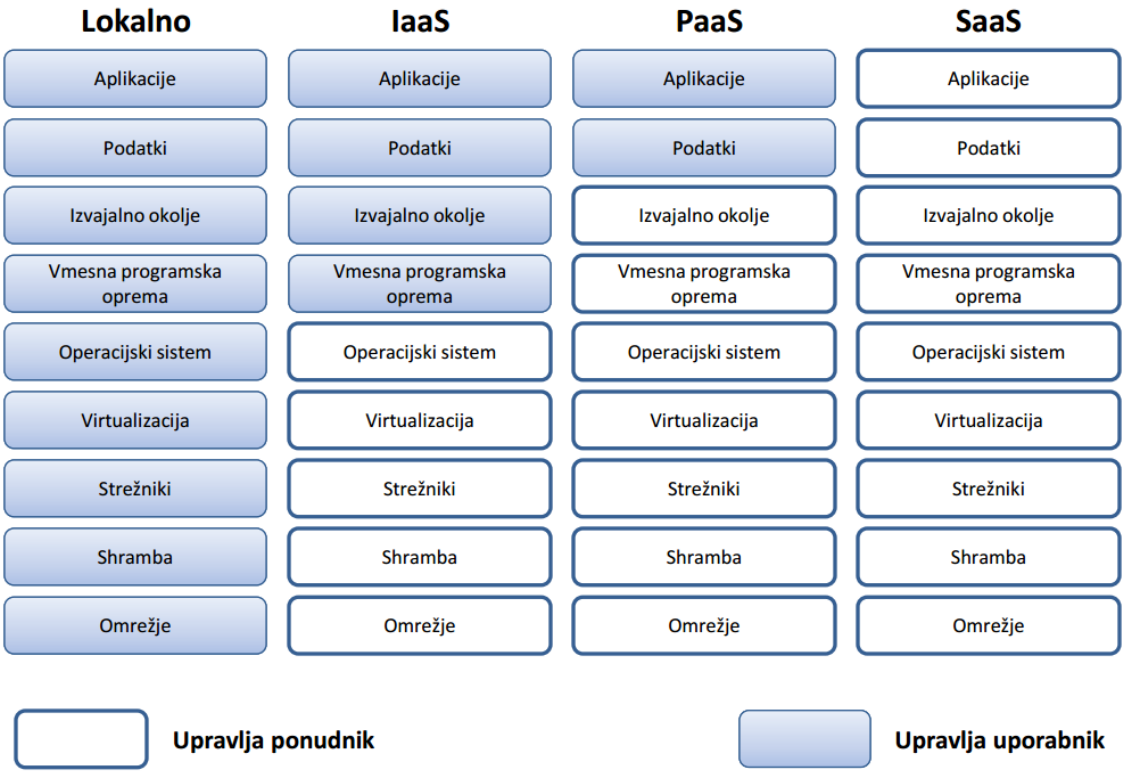
Glede na vrsto storitve v oblaku je lahko storitveni model izveden na tri različne načine:

- **IaaS** – infrastruktura kot storitev:
  ponudnik upravlja uporabo strežnika, operacijksega sistema, virtualizacije;

- **PaaS** – platforma kot storitev:
  že vključuje osnovne dodatne funkcionalnosti (običajno v obliki programskega vmesnika – API), ki jih uporabnik kot platformo uporablja pri razvoju in uporabi lastnih informacijskih rešitev;

- **SaaS** – programska oprema kot storitev:
  pomeni zagotavljanje celotne infrastrukture skupaj s programsko opremo in nastavitvami za njeno delovanje.

Kako si v teh treh načinih ponudnik in upravitelj delita upravljanje oblaka prikazuje Slika 5.



Slika 5: Upravljanje oblaka

Izvedbeni modeli računalništva v oblaku so naslednji:

- **Javni oblaki**:
  Dostopni so javnosti in jih lahko uporablja ter do njih dostopa kdorkoli. Zaradi omejenih možnosti nastavitev varnosti in pogodbenih posebnosti so javni oblaki manj primerni za organizacije, ki upravljajo z občutljivimi podatki.

- **Zasebni oblaki**:
  Dostopni so samo znotraj omrežja organizacije. Zato so vse storitve in infrastruktura pod nadzorom ponudnika, upravljanje pa se lahko izvaja tudi s pomočjo tretjega. Razširljivost storitev je zelo omejena.

- **Hibridni oblaki**:
  So storitve, ki so sestavljene iz več oblakov, tako javnih kot zasebnih oblakov, med seboj pa so povezani z uveljavljenimi tehnologijami.

Na trgu je veliko število ponudnikov teh storitev. Vendar pa ni vsaka rešitev primerna za vsako okolje.

Računalništvo v oblaku obljublja dostopnost do računalniških zmogljivosti iz katere koli lokacije na ekonomičen, prilagodljiv in nadgradljiv način. To pa poraja dvome glede skladnosti z zakonodajo na področju varstva osebnih podatkov in zasebnosti (ZVOP–1). Zlasti javne oblike računalništva v oblaku vzbujajo pomisleke glede varstva osebnih podatkov. Posebne težave pri zagotavljanju pričakovane ravni zavarovanja osebnih podatkov porajajo tudi vprašanja izvoza osebnih podatkov v tretje države, ki ne zagotavljajo enake ravni varstva osebnih podatkov kot domača zakonodaja. Problem je pomanjkanje podatkovnih centrov v Evropi, saj je večina ponudnikov računalništva v oblaku iz ZDA. V času obdobja recesije pa je zelo aktualna dilema tudi zagotovitev kontinuitete poslovanje v primeru bankrota ponudnika. Postavlja se vprašanje, ali in kdaj sploh lahko zaupamo ponudniku računalništva v oblaku, operacijskemu sistemu, strojni opremi, programski opremi [25].

Še ena pomanjkljivost oblačnega shranjevanja je tudi ta, da podatki niso dostopni v fizični obliki takoj, ko bi jih potrebovali. V primeru, da pride do prekinitve povezave z internetom, je varnostna kopija nedosegljiva. Pa tudi drugače je hitrost prenosa kopije pogojena s hitrostjo internetne povezave [23].

2.10 Varnostna tehnologija

Gre za varnostne tehnologije, namenjene tehnični zaščiti pred opisanimi grožnjami informacijskih sistemov. Nanašajo se na različne vidike informacijskega sistema, npr. na omrežja, operacijske sisteme, aplikacijske sisteme (npr. posebna orodja za strežnike SQL za preprečevanje vrivanja SQL (SQL injection)), AAA …

Vendar če osebje ne bo ustrezno usposobljeno in poučeno o varnosti informacij, tudi tako dobra varnostna tehnologija ne bo uspešna proti grožnjam varnosti.

2.10.1 Preverjanje pristnosti, pooblaščanja in vodenje računov

AAA (Authentication, Authorization, Accounting) je temeljni element varovanja informacij, ki pokriva nadzor dostopa do računalniških sistemov. Omogoča prepoznavanje dostopa posameznikov do sistemov, določa, kakšna so njihova pooblastila pri dostopu do določenih lokacij in kaj lahko v sistemih počnejo [1].

Preverjanje pristnosti je postopek, ki določi uporabnikovo identiteto. Pooblaščanje določi, do česa lahko uporabnik dostopa. Vodenje računov pa je orodje, ki preverja in spremlja uporabnikove dejavnosti na računalniškem omrežju.

Preverjanje pristnosti je običajno sestavljeno iz [18]:

- nečesa, kar veste (npr. uporabniško ime in geslo);
- nečesa, kar imate (npr. žetoni ali pametne kartice);
- nečesa, kar ste (biometrija, s katero se preverjajo edinstvene biološke značilnosti, npr. prstni odtisi);
- vašega položaja (npr. ugotavljanje položaja s sateliti za globalno določanje položaja).

2.10.2 Protivirusni programi

To je programska oprema, ki se uporablja za zaščito pred računalniškimi virusi in drugo zlonamerno programsko opremo, kot so črvi, trojanski konji in podobno [15].

2.10.3 Filtriranje vsebine

Orodja za filtriranje vsebine omogočajo filtriranje spleta in filtriranje e-pošte ter tako preprečijo neprimerne informacije (npr. pornografija). S tem je preprečen dostop zaposlenim do takih vsebin.

2.10.4 Požarni zidovi

Požarni zidovi sestavljajo "elektronsko" ograjo okoli računalniškega okolja. Vsebujejo filtre, ki samo določenim vrstam omrežnega prometa dovolijo vstop v omrežje podjetja in zavrnejo vse podatke, ki ne izpolnjujejo določenih meril.

2.10.5 Zaznavanje in preprečevanje vdorov (IDS, IPS)

Sistem IDS za zaznavanje vdorov izvaja nadzor nad prometom v omrežju in spremlja aktivnosti odjemalcev. Na tak način išče vzorce, ki kažejo na možnost izvedbe napada ali pa je do napada že prišlo enkrat v preteklosti.

Sistem IPS za preprečevanje vdorov spremlja aktivnosti v omrežju. Na tak način prepozna škodljive dogodke. Te aktivnosti poskuša zaustaviti oziroma preprečiti. Vse te informacije se tudi beležijo.

2.10.6 Šifriranje

Šifriranje je postopek pretvorbe podatkov v obliko, ki jo nepooblaščena oseba težko prebere.

3 Varnostno kopiranje informacij organizacije "Z"

3.1 Uvod

Zagotavljanje neprekinjenega in nemotenega delovanja informacijskega sistema je temeljnega pomena za poslovanje organizacije "Z". Centralna služba in vodstvo razvijata enotno metodologijo za strokovno in operativno izvedbo postopkov in nudita informacijsko, analitsko, pravno, kadrovsko, finančno, računovodsko in razvojno–organizacijsko podporo. Krog uporabnikov storitev organizacije je širok, od strokovnega osebja do najširše javnosti. Zaradi ogromne količine podatkov, s pomočjo katerih organizacija zagotavlja storitve strankam ob spoštovanju vseh predpisov in ukrepov, ki jih predvideva zakonodaja, se v organizaciji "Z" zavedajo velikih tveganj v poslovanju. Lahko bi prišlo do javnega razkritja zaupnih podatkov, posledično pa bi bil poleg kršitve zakonodaje omajan tudi ugled organizacije. Popolne varnosti sicer ni mogoče doseči, vendar jemljejo zaposleni v organizaciji skrbno vodenje, načrtovanje, izvajanje in vrednotenje varnostnih ukrepov zelo resno in odgovorno.

Pri tem je organizaciji v pomoč njena informacijska varnostna politika. Ta opredeljuje ključne usmeritve in odločitve ter s pomočjo standardov podaja natančna operativna navodila za njeno izvajanje.

Zahteve standarda ISO/IEC 27001 predvidevajo na področju varnosti informacij vzpostavitev mnogih kontrol. To so dokumenti varnostne politike, spremljanje potreb po investicijah, upoštevanje varnostnih zahtev pri načrtovanju novih rešitev oziroma širitvi in nadgradnji obstoječih sistemov, kontrola in preizkušanje pri uvajanju sprememb.

Najprej sledi predstavitev organizacije "Z", njenega poslanstva, vrednot ter vizije, v nadaljevanju pa je predstavljena njena varnostna politika. Ker izvajanje take politike nakazuje potrebo po zanesljivi in zmogljivi opremi, so v organizaciji nujne tudi investicije na tem področju. Vir za podano vsebino je interna dokumentacija organizacije "Z".

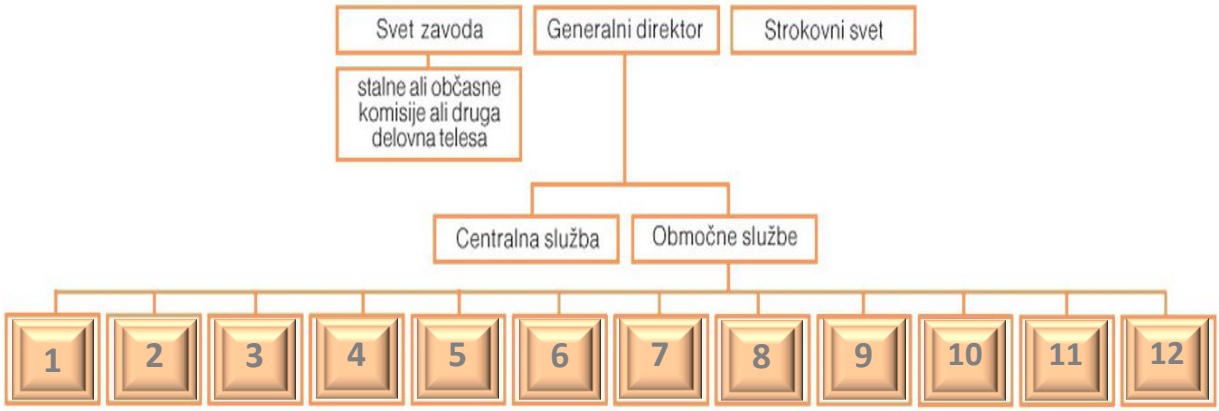
Na osnovi analize tveganj, ki je del učinkovite informacijske varnostne politike, je bilo v organizaciji smiselno uvesti varnostno kopiranje. V nalogi se osredotočimo na tiste kontrole standarda, ki se ob zagotavljanju neprekinjenega poslovanja navezujejo predvsem na varnostno kopiranje. To so smernice za klasifikacijo informacij glede na njihovo vrednost, zakonodajne zahteve, občutljivost in kritičnost, varno in ločeno hranjenje medijev podatkov od mesta kreiranja, redno preverjanje medijev za varnostno kopiranje, pravilen zapis informacij, beleženje in spremljanje napak, postopki za povrnitev v prvotno stanje, urnik izvajanja varnostnega kopiranja, postopki za upravljanje s trakovi pri iznašanju, načrti in postopek za obnovo in vzpostavitev poslovanja po prekinitvi in izvajanje testiranj.

Ker je organizacija na razpotju zaradi dotrajanih sistemov, sledi predstavitev različnih možnosti realizacije varnostnega kopiranja in rezervne lokacije za obnovo po nesreči DR (Disaster Recovery), vključno z možnostjo realizacije teh zahtev organizacije v oblaku. Predstavljene so nejasnosti glede varnosti v oblaku in potrebni predpogoji za prehod v oblak. Argumenti, ki pomembno pripomorejo pri odločitvi glede oblaka, so zagotovo tudi smernice, podane s strani informacijskega pooblaščenca.

Ob proučevanju in vseh prednostih in slabostih različnih rešitev pa se na koncu vseeno pojavlja dvom. Upoštevati je potrebno veliko dejavnikov, proučiti mnogo mehanizmov, analiz, izkušenj, na osnovi katerih je mogoče izbrati in izdelati najugodnejšo rešitev.

3.2 Predstavitev organizacije "Z"

Organizacija "Z" je samostojna pravna oseba s statusom javnega zavoda, ki deluje enotno za območje Republike Slovenije. Z dnem 17. 9. 2013 je dovoljeno število zaposlenih med 500 in 1000 javnih uslužbencev. Deluje na treh ravneh: na sedežu organizacije z vodstvom in centralno službo ter območnih službah.



Slika 6: Organigram organizacije ''Z''

Centralna služba in vodstvo razvijata in zagotavljata enotno metodologijo za strokovno in operativno izvedbo postopkov s področja dejavnosti organizacije ter vsem področjem v okviru organizacije nudita informacijsko, analitsko, pravno, kadrovsko, finančno, računovodsko in razvojno-organizacijsko podporo. Območne službe pa opravljajo strokovne in operativne naloge s področja dejavnosti zavoda na svojem območju.

3.2.1 Poslanstvo, vizija in vrednote

Za organizacijo "Z" je značilna stalna skrb za večjo zaposljivost vseh človeških virov in aktivacija vseživljenjskega učenja. Zagotavlja mehanizme, ki bodo strmeli k uravnoteženi pokritosti trga dela.

Uvrščena je med najboljše ponudnike celovitih rešitev na trgu dela v Evropski uniji do leta 2020.

Glavno vodilo organizacije "Z" je zadovoljen uporabnik. Organizacija zagotavlja prijazno uporabnikovo izkušnjo s kakovostnimi storitvami in prijaznimi sodelavci. Z vso odgovornostjo se zaveda svojega pomena za ustanovitelja in za vse partnerje na trgu dela. Gre za razvijanje potencialov posameznika v ustanovi.

Z vlaganjem v informacijsko tehnologijo in v pravilne rešitve se porajajo novi načini delovanja ustanove, ki omogoča rast in izboljšanje servisa, kar pričakujejo tudi uporabniki.

3.2.2 Varnostna politika organizacije "Z"

Varnostno politiko organizacije opredeljuje Splošni akt o varnostni politiki organizacije "Z", ki ureja organizacijske, tehnične in logično–tehnične postopke ter ukrepe za zavarovanje podatkov in zmogljivosti za njihovo obdelavo z namenom, da se prepreči slučajno, nenamerno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba in prav tako tudi nepooblaščen dostop, obdelava, uporaba ali posredovanje osebnih podatkov.

Cilji varnostne politike:

- preprečitev nepooblaščenih dostopov do informacijskih sredstev in informacij ter njihovega uničenja, odtujitve ali razkritja nepooblaščenim osebam zaradi nevednosti ali malomarnosti;
- varovanje zaupnosti, avtentičnosti in celovitosti informacij, programske opreme, omrežnih storitev in podporne infrastrukture;
- omogočanje razpoložljivosti informacij in virov, ko jih pooblaščeni potrebujejo;
- zagotavljanje primerne ravni varovanja celotne infrastrukture, osebja in informacij oz. dostopa do njih;
- dvig zavesti zaposlenih za varovanje informacij ter njihovo stalno usposabljanje o informacijski varnosti;
- zmanjševanje tveganj človeških napak, kraje, prevare ali zlorabe naprav, škode zaradi varnostnih dogodkov, informacijskih varnostnih dogodkov in okvar;
- zagotavljanje skladnosti z zahtevami veljavne slovenske zakonodaje in zakonodaje Evropske unije;
- upravljanje neprekinjenega poslovanja za nujne primere (požar, potres, katastrofe in podobno);
- uvajanje in izvajanje dobre prakse na področju varovanja informacij.

Uslužbenci organizacije se pri poslovanju in opravljanju svojih del in nalog seznanjajo z zaupnimi osebnimi podatki. Ker se vsakršno ravnanje z osebnimi podatki šteje za obdelavo osebnih podatkov, so upravljavci osebnih podatkov in pogodbeni obdelovalci dolžni zagotoviti zavarovanje osebnih podatkov na podlagi zakonodaje. Predvsem je za organizacijo "Z" zelo pomemben Zakon o varstvu osebnih podatkov (ZVOP–1). Poleg tega je potrebno ohraniti zaupnost, celovitost in razpoložljivost podatkov.

Splošni akt o varnostni politiki organizacije "Z" predpisuje tudi načine, kako postopati, da je omogočena odprava težav v najkrajšem času. Prav tako so vzpostavljeni osnovni elementi načrta neprekinjenega poslovanja in kriznega upravljanja za potrebe nadaljevanja poslovnih procesov v omejenem oz. polnem obsegu za primer izrednega dogodka večje razsežnosti. Izvajanje take politike privede do potreb po zanesljivi in zmogljivi opremi, programski in strojni, ter vlaganju v nenehno posodabljanje in iskanje ugodnejših rešitev.

3.2.3 Investicije

Pred načrtovanjem investicij je potreben podroben pregled obstoječega stanja, v katerem je organizacija. V nadaljevanju sledi seznanitev z izzivi in analiza zahtev za tekoče in prihodnja leta. Nato so predstavljene možnosti in odločitve organizacije v smeri investicijskih vlaganj.
Trenutno stanje nakazuje na problematiko dragega podaljševanja garancij, saj je ključnim komponentam, kot je diskovni sistem in sistem za varnostno kopiranje (tračna knjižnica), potekla garancija. Poleg tega organizacija "Z" ne more širiti komunikacijske prepustnosti med svojimi lokacijami in prepustnosti z internetom oziroma bi bil pogoj, da se to doseže, tudi izjemna motiviranost na "politični" oziroma ustanoviteljevi strani.

Izzivi, s katerimi se organizacija sooča, se nanašajo na zagotavljanje čim višjega nivoja glede brezprekinitvenega poslovanja. Poleg tega se količine podatkov za obdelavo in varnostno kopiranje neprestano večajo. Pričetek izvajanja elektronskega dokumentarnega sistema (EDS) v organizaciji "Z" pa prinaša pravo eksplozijo količine podatkov. Izdelava ocen in zahtev glede potrebnih kapacitet v naslednjih letih pa je lahko le okvirna in približna.

Možnosti organizacije o rešitvah so vsekakor v smeri povezav med sistemi za rezervno lokacijo za okrevanje po nesreči ter zagotavljanjem varnostnega kopiranja. Jasno je, da mora sprejeti dolgoročnejšo odločitev tudi glede načina hrambe transakcijskih podatkov in varnostnih kopij.

Ima dve možnosti:

- Nadaljevanje z uporabo sedanje družine diskovnih sistemov, ki omogočajo "strojno" replikacijo podatkov na rezervno lokacijo ter izredno hitro izdelavo varnostnih kopij za kar nekaj višjo nabavno ceno.
- Poceni diskovnimi sistemi v kombinaciji s programskimi rešitvami za replikacijo, s katerimi lahko doseže enako funkcionalnost z izredno za nižjo nabavno ceno in višjimi stroški upravljanja. To drugo možnost lahko na replicirani strani (ki je hkrati rezervna lokacija) uporabi kar v oblaku, kjer bi izvajala tudi varnostno kopiranje.

Odločitev je pretehtala na prvo možnost, vendar organizacija stalno pogleduje tudi v oblak in išče alternative v tej smeri.

3.3 Varnostno kopiranje organizacije "Z"

Varnostna politika organizacije "Z" predvideva izdelovanje varnostnih kopij pomembnih poslovnih informacij na strežnikih z namenom preprečitve njihove izgube in zagotavljanja možnosti njihove povrnitve v primeru potrebe.

Zato ima organizacija po zahtevah kontrolne točke 10.5.1 standarda ISO/IEC 27001 vzpostavljene kontrole na področju varnostnega kopiranja [1]:

- smernice za klasifikacijo informacij glede na njihovo vrednost, zakonodajne zahteve, občutljivost in kritičnost,
- varno in ločeno hranjenje medijev podatkov od mesta kreiranja,
- redno preverjanje medijev za varnostno kopiranje,
- pravilen zapis informacij,

- beleženje in spremljanje napak,
- postopki za povrnitev v prvotno stanje,
- urnik izvajanja varnostnega kopiranja,
- postopki za upravljanje s trakovi pri iznašanju,
- načrti in postopek za obnovo in vzpostavitev poslovanja po prekinitvi,
- izvajanje testiranj.

3.3.1 Namen in cilji varnostnega kopiranja

Namen varnostnega kopiranja v organizaciji "Z" je povrniti določeno stanje sistema in s tem preprečiti izgubo dela ali vseh podatkov oziroma strežnikov. Cilj pa je zagotoviti neprekinjeno poslovanje organizacije, saj že nekajurna prekinitev delovanja katerega koli kritičnega strežnika povzroči težko popravljive posledice.

Zelo pomembno pri varnostnem kopiranju je, da so podatki shranjeni večkrat in za več kopij nazaj. Zelo nevarno bi namreč bilo varnostne kopije vsak dan sproti prepisovati z novo vsebino, saj je lahko prišlo do napake ali okvare že v preteklih dneh in tega do danes ni nihče opazil. V takih primerih lahko problem rešimo le s starejšimi verzijami.

Delovanje organizacije "Z" pokriva več področij:

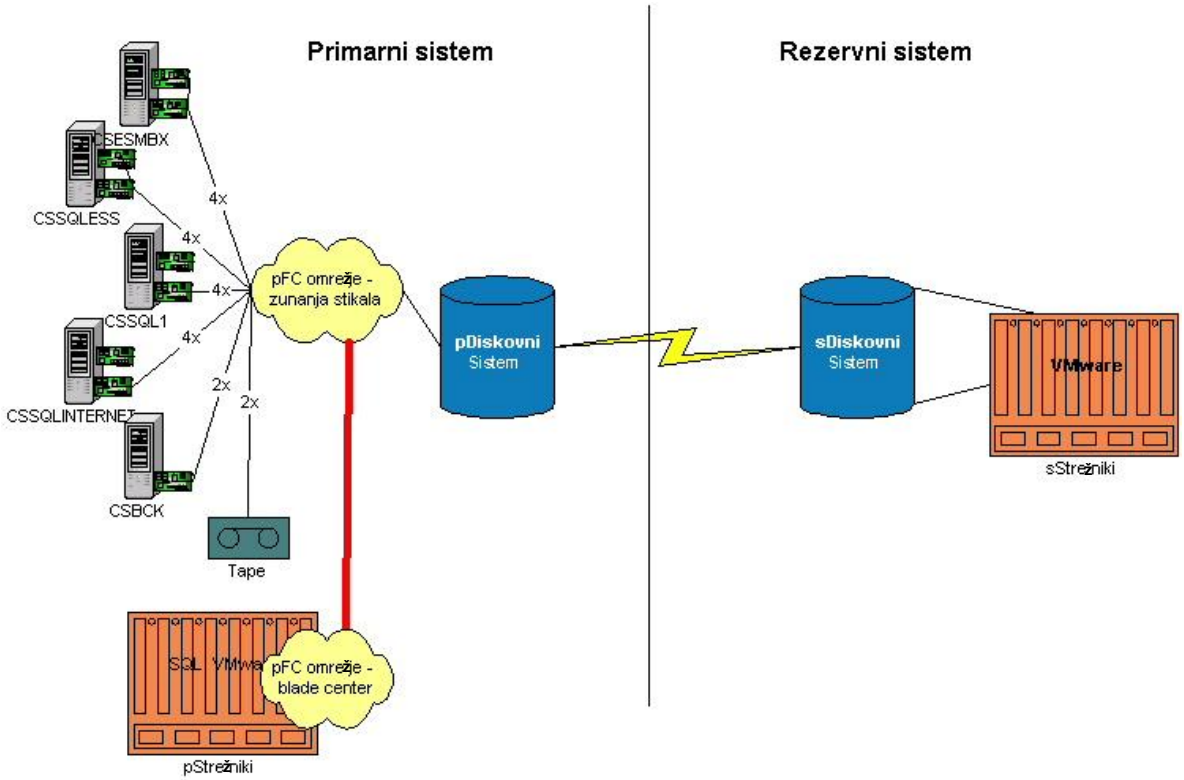
- e-pošta;
- aplikacija "Z1", ki pokriva ključne dejavnosti organizacije in omogoča nemoteno skupinsko opravljanje nalog in izvajanja procesov v realnem času na 400 lokacijah po vsej Sloveniji ;
- aplikacija "Z2", ki omogoča pregled nad vsemi "strankami" ter kontrolo in križanje podatkov organizacije s podatki drugih organizacij javne uprave ter razčiščevanje in ukrepanje pri ugotovljenih odstopanjih;
- vnos PD;
- SOC in Stip;
- kadrovski informacijski sistem, računovodstvo, plače;
- internet v celoti;
- izmenjave podatkov;
- Active Directory;

3.3.2 Tehnologije za izdelavo varnostnih kopij

Za varnostne kopije organizacija uporablja diskovni sistem na primarni lokaciji in rezervni lokaciji s pomočjo zamrznjenih stanj diskovnega sistema v določenih trenutkih (SnapShotov) ter tračno knjižnico (sistem za avtomatsko varnostno shranjevanje na trakove, ki so namenjeni hrambi na oddaljeni lokaciji) in programsko opremo TSM. Hkrati pa diskovni sistem zagotavlja tudi asinhrono replikacijo podatkov za namene rezervne lokacije DR (Disaster Recovery).

Na primarni in rezervni lokaciji je diskovni sistem sestavljen iz dveh sistemov v gruči, kjer je omogočeno izenačevanje obremenitve (load balanced cluster). Strežniki na primarni lokaciji

so klasični, rezine (blade) ter virtualno okolje (VMware). Slednje se nahaja tudi na rezervni lokaciji.



Slika 7: Postavitev primarnega in rezervnega sistema

Za izdelavo varnostnih kopij z opisano opremo ima organizacija na voljo več različnih tehnologij. Odločitev glede izbire je odvisna od politike varnostnega kopiranja:

- na strežnikih z bazami se varnostno kopirajo samo baze, operacijski sistem pa ne;
- varnostnih kopij baz, velikih nekaj 100 GB ali nekaj TB, se ne da učinkovito izvajati brez uporabe tehnologije zamrznjenih stanj diskovnega sistema (SnapShotov) na diskovnem sistemu;
- vsi podatki se kategorizirajo glede časovne kritičnosti za obnovitev (kritični strežniki z bazami) in glede občutljivosti za trajno izgubo podatkov;
- sistem za izvajanje varnostnega kopiranja je TSM in vanj vključene tehnologije;
- finančne omejitve organizacije (licence za TSM so drage, zato se iščejo alternativne rešitve v okviru TSM).

Načini oziroma tehnologije izdelave varnostnih kopij v organizaciji "Z":

- za strežnike, ki so kritični glede časa za povrnitev delovanja se izvajajo zamrznjena stanja diskovnega sistema (SnapShoti);
- posebni TSM moduli za izdelavo varnostnih kopij podatkovnih baz;
- običajni TSM klienti za varnostno kopiranje datotečnih sistemov in datotek (Backup–Archive Client, s pomočjo katerega se naredi varnostna kopija datotečnega sistema na tračno enoto);

- SQL varnostno kopiranje (SQL backup) kot orodje, ki je s strani proizvajalca baze vgrajeno v bazo podatkov v kombinaciji z običajnim TSM klientom, ki lahko datoteko z varnostno kopijo baze shrani v mapo na drugem strežniku oziroma datoteko z varnostno kopijo baze shrani kar neposredno v rezervni sistem (Tivoli TDP za SQL je odlično orodje za varnostno kopiranje, ki omogoča izdelavo SQL varnostne kopije baze podatkov neposredno v rezervni sistem);
- NDMP, ki skrbi za prenos podatkov med napravo NAS (SnapShoti) in tračno knjižnico;
- namenska programska oprema za varnostno kopiranje za virtualna okolja VMware (celovita rešitev predvsem za image level backupe), ki omogoča hitro vzpostavitev ponovnega delovanja v primeru katastrofe in hkrati omogoča deduplikacijo hranjenih podatkov s ciljem zmanjšanja porabe prostora za varnostne kopije;
- replikacije izvaja diskovni sistem (sproži jih strežnik na tak način, da se replicira konsistenten datotečni sistem strežnika oz. diski s konsistentnimi datotekami z bazami podatkov).

3.3.3 Urnik izvajanja varnostnega kopiranja

Organizacija ima izdelano politiko izdelave in hranjenja kopij glede na delitev podatkov po pomembnosti. Ta delitev je stvar dogovora med strokovnimi službami organizacije in službo za informatiko.

Če so podatki kategorizirani kot časovno kritični glede povrnitve, se nahajajo na diskovnem sistemu, replicirajo se na rezervno lokacijo in za zadnjih nekaj dni so popolne varnostne kopije zamrznjenih stanj diskovnega sistema v določenih trenutkih (Snapshoti) na osnovni in rezervni lokaciji.

Vse storitve, za katere se zahteva višji nivo neprekinjenega poslovanja, tečejo na različnih strežnikih:

- Baze se nahajajo na šest različnih produkcijskih kritičnih strežnikih SQL in enem produkcijskem kritičnem strežniku Exchange; baze se replicirajo vsakih 5 minut.
- Za kritične sisteme velja, da se naredi popolne varnostne kopije 1–krat dnevno na diskovnem sistemu, ki se jih replicira še na rezervno lokacijo. Nato se ta varnostna kopija shrani na trak in naslednji dan odnese na tretjo lokacijo.
- Rok hrambe popolnih varnostnih kopij na diskovnem sistemu je 14 dni. Tiste varnostne kopije, ki se iznašajo na trakovih na tretjo lokacijo, pa se hrani drugače (mesečni backup se hrani 3 mesece, letni backup pa 3 leta).

3.3.4 Delitev podatkov

Izguba nekaterih podatkov bi lahko bila usodna za delovanje organizacije, medtem ko je pomembnost nekaterih drugih zadev tako zanemarljiva, da varnostnih kopij zanje ni smiselno delati. Zato organizacija deli podatke glede na 2 kriterija:

- časovno kritični podatki za povrnitev delovanja sistema:

Sistemi so lahko kritični glede časa za povrnitev delovanja v primeru težav ali katastrofalnega dogodka (povrnitev delovanja mora biti realizirana v nekaj urah) ali pa niso kritični in je povrnitev delovanja potrebno vzpostaviti v nekaj dneh ali tednih.

- kritični podatki glede na trajno izgubo:
  Podatki so takšni, da njihova trajna izguba predstavlja za organizacijo nenadomestljivo izgubo, ali pa so takšni, da njihova trajna izguba ni nenadomestljiva oziroma je škoda minimalna. To so na primer podatki, ki jih je mogoče ponovno pridobiti iz nekih drugih podatkov.

Na osnovi kategorizacije podatkov glede občutljivosti za trajno izgubo se nekateri podatki iznašajo na tretjo lokacijo. Gre za večino produkcijskih aplikacij.

3.3.5 Kontrole nad uspešnostjo izdelave varnostne kopije

Za ustvarjene varnostne kopije se je potrebno prepričati, da je bilo opravilo uspešno zaključeno. Računalnik s pomočjo upravljalnika varnostnega kopiranja datotek preveri, ali so bile varnostne kopije uspešno izdelane.

Uspešnost izdelave varnostne kopije in vsebine le-te sproti preverjata operater in njegov pomočnik, ki sta zadolžena za delovanje in spremljanje sistema za varnostno kopiranje s pomočjo transakcijskih dnevnikov varnostnih kopij. Prav tako sta zadolžena za odpravo težav. Organizacija ima tudi sklenjeno pogodbo o pomoči z zunanjim izvajalcem za primer hujših težav.

Poročila o delovanju in težavah se dnevno posredujejo ključnim skrbnikom v informatiki.
Izvajajo se testne povrnitve podatkov zaradi operativnih potreb, zaradi preverjanja uspešnosti postopkov in zato, da strokovnjaka vadita. Te povrnitve vključujejo tudi skrbnike teh podatkov.

3.3.6 Kontrole pri iznašanju trakov z varnostnimi kopijami

Z navodilom za iznašanje in vračanje trakov z varnostnimi kopijami je urejen postopek iznašanja in vračanja medijev z varnostno kopijo podatkov izven strežniškega centra organizacije na zunanjo lokacijo.

Varnostne kopije se hranijo na za to določenih mestih, ki morajo biti ognjevarna, zavarovana proti poplavam in elektromagnetnim motnjam, v okviru predpisanih klimatskih pogojev ter zaklenjena.

Del varnostnih kopij, ki vsebuje podatke, katerih izguba bi pomenila za organizacijo "Z" nenadomestljivo škodo, se prepiše na medije, ki so namenjeni hrambi na drugi lokaciji. Sistem za izdelavo varnostnih kopij samodejno pripravi medije za iznos. Požene se samodejno opravilo, ki pošlje sporočilo s seznamom medijev za iznos na drugo (offside) lokacijo. Sporočilo dobita operater in hranitelj medijev. Operater pobere iz knjižnice medije s seznama in jih pripravi za transport. Enako sporočilo se kreira tudi za medije na lokaciji offside, ki se morajo vrniti nazaj v sistem za izdelavo varnostnih kopij podatkov. Na sistemu

se tem medijem nastavi status "vault". Prejete medije pa operater nemudoma vstavi v knjižnico.

Podatki na varnostnih kopijah (offsite backupi) se hranijo v prostoru s strežniki v ognjevarni omari. Prostor je dostopen samo službi za informatiko in hranitelju medijev ter je klimatiziran.

Medije prenaša vsak delovni dan kurir iz lokacije strežniškega centra na drugo lokacijo in nazaj v posebej za to namenjenem transportnem kovčku. Zaradi narave delovanja samodejnih procedur lahko občasno pride do situacije, da je npr. zaradi praznika dela prost dan, samodejne procedure pa vseeno pripravijo vse potrebno za iznos in vračanje trakov. V tem primeru se na prvi naslednji delovni dan smiselno uporabijo ta navodila za vse pripravljene medije in sezname, ki so nastali od prejšnje izvedbe tega postopka.

Operater in hranitelj vsak zase vodita evidenčno mapo z nazivom "Evidenca prejetih in vrnjenih medijev – operater" oziroma "Evidenca prejetih in vrnjenih medijev – hranitelj", v katero odlagata dnevna izpisana in podpisana elektronska sporočila s seznami medijev. Kurir in operater preverita, da so v kovčku res tisti mediji, ki so na seznamu za iznos. Enak postopek velja med kurirjem in hraniteljem. Če se seznam in vsebina razlikujeta, to uredi operater tako, da dobi kurir skladen seznam in kovček.

Zap. št.	Opravilo	Kdo	Kdaj (vsak delovni dan)	Kje
1.	**Priprava medijev za iznos na drugo lokacijo in pošiljanje poročila o medijih za iznos in povratek v sistem.**	Sistem za izdelavo varnostnih kopij	do 9:30	Strežniški center
2.	**Preverjanje uspešnosti pošiljanja poročila o medijih**	Operater varnostnih kopij	do 9:30	Strežniški center
3.	**Izločanje novih medijev iz knjižnice**	Operater varnostnih kopij	do 9:30	Strežniški center
4.	**Priprava starih medijev za predajo kurirju**	Hranitelj medijev	do 14:00	Druga lokacija
5.	**Predaja novih medijev kurirju**	Operater varnostnih kopij Kurir	do 9:30 oz. odhoda kurirja	Strežniški center
6.	**Transport in predaja novih medijev hranitelju**	Kurir Hranitelj medijev	do 14:00	Pot Druga lokacija
7.	**Predaja starih medijev kurirju**	Kurir Hranitelj medijev	do 14:00	Druga lokacija
8.	**Odložitev novih medijev v hrambo**	Hranitelj medijev	do 15:00	Druga lokacija
9.	**Transport in predaja starih medijev operaterju**	Operater varnostnih kopij Kurir	do 15:00	Pot Strežniški center
10.	**Vstavljanje starih medijev v knjižnico**	Operater varnostnih kopij	do 15:00	Strežniški center
11.	**Nadzor izvajanja postopka**	Vodja operaterja	občasno	Strežniški center Druga lokacija

Tabela 1: Seznam opravil pri iznašanju trakov

Vodja operaterjev občasno preveri izvajanje postopka v ključnih elementih:

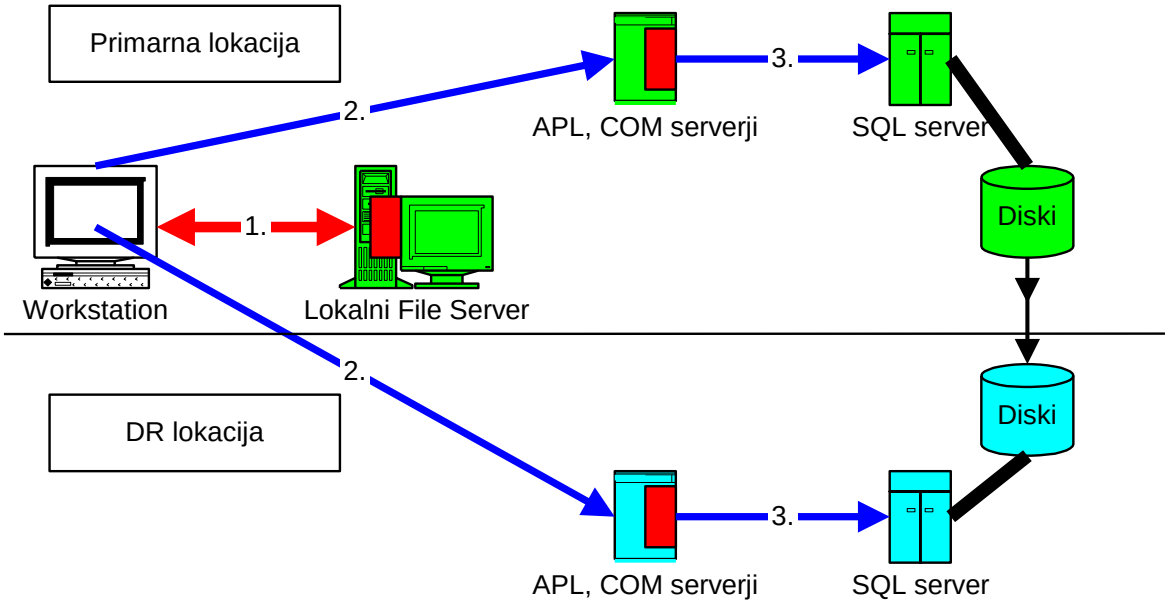
- da se mediji dnevno prenašajo,

- varovanje medijev na poti,
- vsebina evidenčnih map.

O pregledu pripravi zapis in ga posreduje operaterju za hrambo v evidenčni mapi, hkrati ga posreduje v vednost tudi lastniku procesa. V primeru odstopanj od postopkov, opredeljenih v tem navodilu, vodja operaterja sprejme ustrezne ukrepe.

3.3.7 Povrnitev delovanja v kritičnih situacijah

S pomočjo DR lokacije in varnostnih kopij lahko organizacija s čim manj stroški in čim hitreje obnovi izgubljene podatke. Pri povrnitvi strežnikov z bazami, ki niso kritični glede časa za povrnitev delovanja, se povrne samo baze s podatki. Za tiste, ki so kritični, pa se vzdržujejo stalno delujoči virtualni strežniki, ki se jim po potrebi samo priključijo zadnje aktualne kopije podatkovnih baz.



Slika 8: Koncept povrnitve delovanja preko rezervne DR lokacije

Osnovni koncept povrnitve delovanja kritičnih storitev organizacije, prikazan na Sliki 7, je sledeč:

- na rezervne virtualne podatkovne strežnike se priključi zadnje stanje baz podatkov pred katastrofalnim dogodkom, ki so replicirane na DR lokaciji;
- preklop časovno kritičnih storitev se izvede na virtualno infrastrukturo, ki je v stalni pripravljenosti (nonstop) na DR lokaciji;
- klientom se nadomesti konfiguracijske datoteke za dostop do aplikacij (na lokalnih File Serverjih) z DR verzijami, kar naj bi se izvedlo samodejno ob ročno proženem signalu na centralni lokaciji; zamenjava konfiguracijskih datotek traja 15 minut;
- nujno je potrebno nadomestiti izraze, kot je File Server z datotečnim strežnikom;
- klienti morajo ponovno pognati vse aplikacije za kritične storitve.

3.4 Predlog selitve varnostnih kopij v oblak

Zaradi potreb po zmanjševanju investicij, hkrati pa zaradi zagotavljanja čim bolj primerljive RTO in RPO ob minimalnem povečanju tekočih stroškov je nastala ideja o selitvi lokacije DR v oblak.

Organizacija "Z" je zaradi dotrajanih sistemov pred pomembnimi odločitvami, kako rešiti problematiko varnostnega kopiranja. Neprestano se veča tudi količina podatkov. Možnosti organizacije so vsekakor v smeri povezav med sistemi za rezervno DR lokacijo ter zagotavljanjem varnostnega kopiranja. Organizacija mora sprejeti dolgoročno odločitev glede načina hrambe transakcijskih podatkov in varnostnih kopij.

Tu ima možnost nadaljevanja uporabe sedanje družine diskovnih sistemov, ki omogočajo "strojno" replikacijo podatkov na rezervno DR lokacijo ter izredno hitro izdelavo varnostnih kopij za kar nekaj višjo nabavno ceno. Takšno funkcionalnost lahko doseže tudi z izredno poceni diskovnimi sistemi v kombinaciji s programskimi rešitvami za replikacijo za nižjo nabavno ceno in višjimi stroški upravljanja.

To drugo možnost lahko na replicirani strani (ki je hkrati lokacija DR) uporabi kar v oblaku, kjer bi izvajala tudi varnostno kopiranje. Ponudnikov teh storitev je na tržišču zelo veliko. V organizaciji so se odločili, da ustreznost oblačnih storitev najprej preverijo s ponudnikom Microsoft. Razlogi za to so bili:

- uporaba MS Office za pisarniško delo, ki v oblaku ponuja nekatere enostavne prednosti;
- za enostavno rešitev problema stroškov z lastnim sistemom za e–pošto Exchange je v oblaku dostopen tudi sistem za razširjeno komuniciranje (Lync);
- Microsoft nudi v oblaku storitve PaaS in IaaS, ki bi bile brez velikih težav neposredno uporabne za organizacijske informacijske rešitve.

Tako se je začel pregled storitev Microsoft Office 365. Družba KPMG, poslovno svetovanje, je opravila revizijo oblačne ponudbe Office 365 in platforme Azure v naslednjem obsegu:

- pregled doseganja, certificiranja skladnosti z varnostnimi standardi za storitve v oblaku;
- pregled dokumentacije in dokazov o praksah pri zagotavljanju varnosti in razpoložljivosti storitev v oblaku;
- pregled načinov zagotavljanja skladnosti z Zakonom o varstvu osebnih podatkov s spremembami in dopolnitvami glede varnosti in zasebnosti osebnih podatkov.

Kot izhaja iz opisov v dokumentaciji, je bil namen pregleda vzpostavljenih kontrol in stanja delovanja storitev v oblaku Microsoft Office 365 ta, da ugotovijo skladnost z varnostnimi standardi ter skladnost z zakonodajo s področja varovanja osebnih podatkov.

3.4.1 Varnostne kopije podatkov v oblakih

Velik potencial oblačnega računalništva je tudi organizacije javne uprave privedel do tega, da v svojih strateških načrtih vključujejo možnost postopnega prehoda v oblak. Seveda je prehod v oblak zelo kompleksen projekt z mnogimi pomisleki. Zato je mogoče bolj smiselno s

storitvami v oblaku začeti kot možnostjo rezervne rešitve v primeru nesreče. Z razvojem oblačnega računalništva pa tudi čedalje več ponudnikov oblačnih storitev omogoča izdelavo varnostnih kopij podatkov kot alternativo današnji klasični izdelavi [24].

Prednosti izdelave varnostne kopije v oblaku:

- prilagodljivost oblaka našim potrebam glede performans;
- velik razpoložljiv prostor za shranjevanje in stroški, ki se obračunavajo glede na dejansko uporabo virov;
- uporaba oblaka lahko dodatno poenostavi lastno informacijsko infrastrukturo, ker ni več potrebe po lastnem upravljanju hrambe podatkov.

Pomanjkljivosti [25]:

- prenos podatkov v oblak oziroma iz njega je omejen s pasovno širino spleta, ki onemogoča hiter prenos velike količine podatkov;
- pri pogodbeni obdelavi podatkov se pojavljajo dvomi glede zaupanja v varnostne postopke in ukrepe, zanesljivost, dostopnost in stanovitnost oblačnega obratovanja;
- posebne težave pri zagotavljanju pričakovane ravni zavarovanja osebnih podatkov porajajo tudi povezana vprašanja iznosa osebnih podatkov v tretje države, ki ne zagotavljajo enake ravni varstva osebnih podatkov kot domača zakonodaja.

3.4.2 Varnost v oblaku

Ravno varnost podatkov v oblaku je največkrat obravnavana problematika strokovnjakov. Dejstvo je, da se napadi in vdori množijo, delovanje oblaka pa ni brez vrzeli, kar napadalci tudi s pridom izkoriščajo.

Varnostne kopije podatkov morajo biti pri ponudniku kriptirane. Ključ ima stranka, brez njega dostop do podatkov ni mogoč. Seveda mora imeti ponudnik kopijo podatkov tudi na drugem diskovju na drugi lokaciji in okrevalni načrt za storitev, ki jo ponuja. Ponudnik mora imeti tudi mehanizem, ki mu omogoča preverjanje kvalitete varnostnih kopij in zaznavanje morebitnih težav ali neskladij.

Poleg tega mora nadzor nad informacijsko varnostjo pri ponudniku oblačnih storitev preveriti:

- da so produkcijski podatki zaščiteni;
- da so produkcijski sistemi nadzorovani in omogočajo zaščito pred varnostnimi grožnjami in prekinitvijo razpoložljivosti informacij;
- da so logični dostopi do sistemov in podatkov omejeni;
- da so spremembe produkcijskih sistemov primerno vodene za minimiziranje verjetnosti prekinitve delovanja in nepooblaščenih sprememb.

3.4.3 Smernice informacijskega pooblaščenca

Smernice informacijskega pooblaščenca podajajo praktične napotke upravljavcem zbirk osebnih podatkov. Na najpogostejša vprašanja s področja varstva osebnih podatkov poskušajo

odgovoriti na jasen, razumljiv in uporaben način. S pomočjo smernic naj bi upravljavci dobili priporočila, kako naj v praksi zadostijo zahtevam Zakona o varstvu osebnih podatkov [16].

Vsakršno ravnanje z osebnimi podatki se šteje za obdelavo osebnih podatkov. Osebni podatki pa so vsi podatki, ki se nanašajo na določenega posameznika. Pri uporabi računalništva v oblaku so najbolj izpostavljeni naslednji trije vidiki varstva osebnih podatkov [25]:

- pogodbena obdelava osebnih podatkov,
- zavarovanje osebnih podatkov,
- iznos osebnih podatkov v tretje države.

Pooblaščenec opozarja, da gre za obdelavo osebnih podatkov tudi v situacijah, ko pogodbeni obdelovalec ne ve, na koga se podatki nanašajo. Prav tako gre za obdelavo osebnih podatkov in zakonske dolžnosti, če zunanji ponudnik hrani podatke na svojih diskovnih zmogljivostih v kriptirani, zunanjemu ponudniku hrambe neberljivi obliki. Zato se pojavlja vprašanje, ali in kdaj lahko zaupamo zunanjemu ponudniku računalništva v oblaku. Vsekakor je bistvena transparentnost storitev računalništva v oblaku in opravljena analiza tveganj. Naročniku mora biti jasno predstavljeno, kako bo zagotovljena zaupnost, celovitost in razpoložljivost hranjenih podatkov [25].

Posebna pozornost, na katero opozaja pooblaščenec, je vprašanje izvoza osebnih podatkov v tretje države. Organizacija lahko osebne podatke, s posebnim dovoljenjem pooblaščenca, posreduje v tretjo državo, kadar ta zagotavlja ustrezno raven varstva osebnih podatkov. Ker največ ponudnikov oblačnih strotitev prihaja iz ZDA, njihov režem pa se precej razlikuje od evropskega, skrbijo za lažjo izmenjavo in spoštovanje medsebojne odgovornosti, načela Varnega pristana. Vendar niti to ni zagotovilo za upoštevanje vseh varnostnih ukrepov s strani ponudnika [25].

Pooblaščenec opozarja glede računalništva v oblaku še na nekatera pomembna tveganja [25]:

- potenciali računalništva v oblaku so izjemni, vendar pa zaradi tega ne sme priti do nižanja ravni varstva osebnih podatkov kot temeljne človekove pravice;
- vloženi morajo biti nadaljnji napori v raziskave, standardizacijske in certifikacijske sheme in prilagoditve zakonodajnega in regulativnega okvira za dvig stopnje zaupanja v storitve računalništva v oblaku;
- upravljavci osebnih podatkov morajo pred uporabo storitev računalništva v oblaku izvajati potrebne analize tveganja in presoje vplivov na zasebnost, po potrebi s pomočjo zaupanja vrednih tretjih strank;
- ponudniki storitev računalništva v oblaku morajo zagotoviti večjo transparentnost svojih praks, predvsem pa zagotovil s področja informacijske varnosti;
- nadzorni organi na področju varstva osebnih podatkov in zasebnosti morajo nadaljevati z oblikovanjem smernic in ozaveščanjem glede vprašanj varstva osebnih podatkov in zasebnosti.

3.4.4 Rešitve o lokaciji DR v oblaku

Organizacija "Z" poseduje ogromne količine podatkov v elektronski obliki in že znotraj nje je potrebno veliko discipline pri nadzoru, kdo je podatke uporabljal in kdaj, četudi vemo, kdo vse ima dostop do njih. Poleg tega vsaka rešitev tudi ni primerna za konkretno problematiko. Tako je na primer od uporabljene platforme odvisno, kakšne nove poslovne ideje so sprejemljive.

Ponudniki oblačnih storitev omogočajo shranjevanje podatkov v oblaku na veliko različnih načinov. Problem, ki se pri organizaciji "Z" pojavlja že takoj na začetku je, kako spraviti svoje operativne podatke z minimalno zamudo (največ nekaj minut) v oblak.

Ena izmed rešitev zahteva poseben namenski diskovni sistem. Ta deluje kot običajno skladišče (storage), en del pa glede na konfiguracijo samodejno replicira v oblak. Omenjena rešitev bi bila sprejemljiva, ampak bo ta produkt v Sloveniji na voljo šele v tekočem letu.

Brez zgoraj omenjenega diskovnega sistema je potrebno poskrbeti za replikacijo SQL baz v oblak z uporabo mehanizmov, vgrajenih v baze podatkov.

Ena možnost je, da se postavi raztegnjena gruča (Stretch cluster), ki ima možnost preklopa na oblačni strežnik tudi brez ročne intervencije. Naslednje možnosti temeljijo na replikacijskih zmogljivostih MS SQL, ki so predvsem zrcaljenje zbirke podatkov (Database Mirroring), Log Shipping in obnovitev iz varnostne kopije (Backup/Restore). Najbolj zanimivi sta prvi dve.

Dodatno je organizacija ugotovila, da bi za tekoče repliciranje podatkov lahko imela v oblaku relativno manj zmogljive strežnike, kar bi pomenilo nižje mesečne stroške. Potrebno pa bi bilo v oblaku nadgraditi sedanji Active Directory, kar bi pomenilo dodaten domenski kontroler v oblaku.

Za tako postavitev bi za 8 majhnih oblačnih strežnikov mesečno plačevali cca 300 € + DDV. To je cena rezervne DR lokacije, ki ni v uporabi. V primeru rezervne lokacije DR bi teh 8 DR strežnikov nadgradili s procesorji in RAM–om ter bi tako za maksimalno varianto plačevali cca 5000 €/mesec (po minutah uporabe).

Posebno poglavje je omrežje. Virtualni strežniki bi bili v oblaku vidni kot posebna nova lokacijska enota organizacije, ki bi bila popolnoma zaprta za javno omrežje, kar je v konfiguraciji sistema v oblaku zelo enostavno izvedljivo. To se naredi s približno 10 kliki. Potem bi HKOM (prostrano omrežje državnih organov) vzpostavil povezavo VPN (Virtual Private Network) do te oblačne strani na enak način kot do ene območne enote. Za povezavo do strežnikov v oblaku bi uporabili kar sedanjo komunikcijsko povezavo, ki bi bila zaradi replikacije sicer bistveno bolj obremenjena, a pri tem bi vsaj delno olajšanje omogočila kompresija komunikacijskega prometa zaradi replikacije.

Varnostne kopije bi bilo mogoče delati na repliciranih podatkih, ki so v oblaku, in nato te kopije tam tudi hraniti (2 oddaljeni lokaciji), kar bi bilo zelo dobro tudi za potrebe EDS (elektronskega dokumentarnega sistema).

Nedoločen pa je način take izvedbe in cena hrambe varnostnih kopij v oblaku. SQL agent na strežniku, ki združuje in terminsko razporeja posamezna opravila, ki naj jih opravlja strežnik SQL, bi verjetno moral v izvajanju časovnih opravil (jobs) prekiniti operacijo, v tem primeru

replikacijo. Nato pa bi moral SQL agent narediti varnostno kopijo oblačnega SQL na neko drugo lokacijo v oblaku. Za restavriranje ene tabele bi bilo potrebno z interneta vleči celo bazo. V oblaku bi morali imeti tudi replicirane kopije nekaterih strežnikov, ki nimajo baz podatkov, kot so na primer aplikacijski in spletni strežniki. Organizacija je ugotovila, da za tako funkcionalnost trenutno ne obstaja boljša rešitev, kot je varnostno kopiranje in povrnitev delovanja (backup/restore).

Za povrnitev delovanja je postopek naslednji:

- Povrne se lahko delovanje podatkovnih strežnikov, katerih podatki se replicirajo na rezervno DR lokacijo. V ta namen so na rezervni lokaciji v pripravljenosti delujoči strežniki z operacijskim sistemom in isto verzijo SQL (MS SQL 2008 R2), kamor se restavrirajo sistemske baze (msdn, master). Kopije teh baz se shranjujejo na diske strežnika na primarni lokaciji, nato pa se ti diski replicirajo na rezervno DR stran. Nazadnje se izvede še priklop baz, ki se nahajajo na repliciranih diskih rezervne DR strani.

- Z orodji iz družine TSM se lahko povrne celotne aplikacijske strežnike, ki so vsi virtualni.

- Povrnitev neke baze podatkov ali ene tabele iz baze, pri čemer primarni strežnik še deluje, se izvede glede na tehnologijo, s katero je bila varnostna kopija narejena. To se zgodi v primeru, ko nekdo pomotoma pobriše nek podatek iz baze podatkov in je potrebno povrniti samo tisti podatek. Razlika je pravzaprav samo v izgledu grafičnega vmesnika in kam se ta povrnitev izvede. Organizacija za te namene uporablja tehnologijo data protection module za TSM, SnapManager ali pa navaden MS SQL backup.

Organizacija je ugotovila, da vseh sistemov ne namerava seliti v oblak. Za preostale sisteme bi torej morala vzpostaviti primerne sisteme za hrambo transakcijskih podatkov in delovanje strežnikov, hkrati pa zagotoviti tudi varnostne kopije teh sistemov, ki bi delovali izven oblaka. In tu se organizacija ponovno sooči s svojo zastarelo in po kapacitetah premajhno tračno knjižnico in diskovnim sistemom.

Dodatna težava pri delnem prehodu organizacije v oblak so komunikacijske težave v zvezi z omrežjem HKOM (propustnost, možnost vzpostavitve oddaljene lokacije v oblaku) ter pravne in varnostne omejitve.

3.5 Odločitve o ustreznosti rešitve

Ob pregledu vseh prednosti in slabosti različnih rešitev je potrebno upoštevati veliko dejavnikov, proučiti mnogo mehanizmov, analiz in izkustev, na osnovi katerih je mogoče izbrati in izdelati najugodnejšo rešitev.

Izzivi s katerimi se organizacija sooča, se nanašajo na zagotavljanje čim višje brezprekinitvenega poslovanja. Poleg tega pa pričetek izvajanja EDS v organizaciji "Z" prinaša pravo eksplozijo količine podatkov.

Pri sedanjem, utečenem načinu, je potrebno upoštevati, kolikšen finančni zalogaj predstavlja vzdrževanje za organizacijo. Opremljen je bil primeren prostor s strežniki, diskovjem in drugimi komponentami, ki omogočajo nemoteno delovanje kompletnega računalniškega sistema. Ustrezno usposobljeni zaposleni morajo skrbeti in obvladovati zelo obsežno in kompleksno strukturo informacijskega prostora in biti v vsakem trenutku pripravljeni na obvladovanje katere koli kritične situacije. Dejstvo je, da se količine podatkov ves čas povečujejo, kar predstavlja za organizacije tudi povečevanje stroškov. K vsemu temu je potrebno prišteti še stroške programske opreme z licencami in strošek porabljene električne energije za naprave (strežniki, klime itd.), ki delujejo neprekinjeno 24 ur na dan.

Nekatere različice programov in funkcij so čedalje bolj vezane na oblak in druge verzije enostavno sploh niso na razpolago (npr. Office na zahtevo). Torej gre za načrtovano usmerjanje v oblačne storitve. Poleg tega je trženje licenc na način najema namesto nakupa čedalje dražje s ponavljajočimi se stroški in omejenostjo na eno napravo.

Oblačne storitve sicer imajo svoje prednosti, saj so povsem neodvisne od lokalnega sistema. To pomeni varnost v primeru kraje, ujme, fizične odpovedi. Po drugi strani pa v primeru povrnitve celotne baze ali strežnika, ki ima varnostno kopijo v oblaku, lahko takšna operacija traja dneve ali celo tedne, ker je hitrost komunikacijske povezave do oblaka bistveno bolj omejena kot v lokalnih omrežjih. Hitre širokopasovne povezave pa zopet predstavljajo dodaten strošek. Zato lokalna kopija pri ponudniku lahko pomeni razliko med nekajurnim ali nekajdnevnim izpadom poslovanja organizacije [10].

V organizaciji se standardi varstva podatkov v primerjavi s tradicionalno obdelavo podatkov zaradi računalništva v oblaku ne smejo znižati. Ponudniki oblačnih storitev sicer zagotavljajo certifikate o varstvu podatkov in spoštovanju slovenske zakonodaje, vseeno pa skrb za doslednost in ustreznost zavarovanja osebnih podatkov pred zlonamernim vohljanjem po podatkih, še vedno ostaja na naročnikovi strani.

Argumenti, ki pomembno pripomorejo pri odločitvi organizacije "Z" glede oblaka, so zagotovo tudi smernice, podane s strani informacijskega pooblaščenca.

Jasno je, da mora organizacija sprejeti dolgoročno odločitev glede načina hrambe transakcijskih podatkov in varnostnih kopij. Tu ima dve možnosti:

- Uporaba sedanje družine diskovnih sistemov še naprej. Ti omogočajo "strojno" replikacijo podatkov na rezervno DR lokacijo ter izredno hitro izdelavo varnostnih kopij z višjo nabavno ceno.
- Podobno funkcionalnost lahko doseže z izredno poceni diskovnimi sistemi v kombinaciji s programskimi rešitvami za replikacijo z nižjo nabavno ceno in višjimi stroški upravljanja. To možnost lahko na replicirani strani (ki je hkrati lokacija DR) uporabi kar v oblaku, kjer bi izvajala tudi varnostno kopiranje.

4 Zaključek

Ugotovili smo, da so lahko država in njeni javni zavodi učinkoviti le tako, da prvič delujejo po načelih zakonodaje in drugič, da zagotovijo neprekinjeno delovanje. Pri tem je bistvenega pomembna obvladovanja tveganj in informacijska varnost, ki jo organizacije vzpostavljajo s pomočjo varnostnih mehanizmov. Osrednje mesto naloge je bilo namenjeno varnostnemu kopiranju podatkov, ki poleg ostalih varnostnih mehanizmov v primeru kritične situacije ključno pripomore k nadaljevanju poslovanja organizacije, če ne na primarni, pa na rezervni lokaciji.

V prvem delu naloge smo zaradi razumevanja samega področja informacijske varnosti predstavili družino standardov ISO/IEC 27000, ki prispevajo k ustvarjanju varnostne politike organizacije. Seznanili smo se z dogodki in dejavnostmi, ki ogrožajo varnost podatkov ter predstavili načine, ki se jih organizacije poslužujejo pri zmanjševanju tveganj in katere tehnologije so jim pri tem v pomoč.

V drugem delu smo predstavili organizacijo "Z" in realizacijo varnostnega kopiranja podatkov v organizaciji. Po zahtevah standarda ISO/IEC 27001 ima organizacija na področju varnostnega kopiranja informacij vzpostavljenih več kontrol, od delitve na kritične podatke glede izgube in delitve glede kritičnosti za povrnitev delovanja v kritičnih situacijah, do dnevnih kontrol nad uspešnostjo izdelave varnostne kopije in kontrol glede iznašanja trakov. Ker je organizacija na razpotju zaradi dotrajanih sistemov, išče alternativne možnosti izvedbe varnostnega kopiranja in rezervne lokacije za obnovo v primeru nesreče. Podrobneje smo obdelali ustreznost oblačnih storitev za potrebe organizacije.

Uvajanje neke nove, celovite rešitve, v našem primeru oblačnega poslovanja, je zahteven projekt. Organizacija mora ves čas delovati tako, da komitenti ne občutijo nobenih težav. Če so zastavljeni roki kratki, se zahtevnost še poveča. Marsikateri zaposleni mora biti pripravljen dati vse od sebe za uspešno uvedbo novega sistema.

Načrti in izdelava zahtev glede potrebnih kapacitet v naslednjih letih je zahtevno delo. Predvidevanja so lahko le okvirna in približna. Oprema in sistem mora omogočati agilnost in sprotno prilagajanje.

Spoznali smo, da je velika prednost notranjega (tradicionalnega) zagotavljanja nadzora ta, da lahko organizacija sama poskrbi za varnost s pomočjo varnostnih mehanizmov in vzpostavljenim sistemom varnostnih kontrol. Pomembna razlika notranjega izvaja varnosti od zunanjega (oblačnega) je tudi ta, da gre pri zunanjem izvajalcu za zaupanje v celoti, kar ne vključuje le zaupanja v varnostne postopke in ukrepe, temveč gre tudi za zanesljivost, dostopnost in stanovitnost obratovanja. Cene oblačnih storitev so zelo nejasno definirane, še posebej, ko gre za pogled v daljnjo prihodnost. Nejasna in dvoumna so pravila o vpogledu v podatke.

Odločitev je tako pretehtala na možnost nadaljevanja uporabe sedanje družine diskovnih sistemov, ki omogočajo "strojno" replikacijo podatkov na rezervno lokacijo ter izredno hitro izdelavo varnostnih kopij. Uporaba diskovnih sistemov ima namreč pomembno prednost v krajših časih operacij ter boljšo strategijo okrevanja po nesreči.

Kljub temu organizacija aktivno spremlja razvoj storitev v oblaku in presoja o primernosti prehoda v oblak. Pri tem je varnost seveda na prvem mestu.

Seznam slik

Seznam tabel

Literatura

[1] Košćak D. (2011), Varovanje informacij v skladu s standardom ISO/IEC 27000. Diplomsko delo, Fakulteta za računalništvo in informatiko, Univerza v Ljubljani.

[2] Rakovec S. (2005), Varovanje informacij skladno s standardom BS 7799. Diplomsko delo, Fakulteta za računalništvo in informatiko, Univerza v Ljubljani, pogl. 4.

[3] Vidmar T. (2002), Informacijsko – komunikacijski sistem, Ljubljana: Založba Pasadena, pogl. 11, 15.

Internetni viri:

[4] Buček S. (2010), Primer uporabe dwdm optičnega prenosnega sistema cisco ons 15530. Dostopno 20.2.2014 na: https://www.src.si/library/includes/file.asp?FileId=22

[5] Disaster recovery tako ali drugače (2012). Dostopno 17.12.2013 na: http://www.lancom.si/uploads/media/DisasterRecovery_TakoAliDrugace.pdf

[6] Enotne tehnološke zahteve (2011). Dostopno 22.12.2013 na: http://www.arhiv.gov.si/fileadmin/arhiv.gov.si/pageuploads/zakonodaja/ETZ_2.0_-_2.del_razlicica_2.0.pdf

[7] Gleich D., Čučej Ž. (2004), Varnost informacij in omrežij. Dostopno 28.12.2013 na: http://improvet.cvut.cz/project/download/C2SI/Varnost_informacij_in_omrezij.pdf

[8] ISO/IEC 27000 (2013). Dostopno 16.12.2013 na: http://en.wikipedia.org/wiki/ISO/IEC_27000-series

[9] Kadri so ključni člen za varnost organizacije (2013). Dostopno 11.12.2013 na: http://www.dnevnik.si/poslovni/gazele/kadri-so-kljucni-clen-za-varnost-organizacije

[10] Ko bomo prestali to krizo, bomo prav zaradi nje veliko boljši (2012). Dostopno 4.1.2013 na: http://www.src.si/library_si/pdf/infosrc/2012-69/infoSRC69.pdf

[11] Praktični vidiki vpeljave sistema upravljanja informacij (SUVI) (2010). Dostopno 21.12.2013 na: http://www.dsi2010.si/upload/predstavitve/Informacijska%20varnost%20in%20upravljanje%20tveganj/ZELE%20PRAKTICNE%20IZKUSNJE%20PRI%20VPELJAVI%20IN%20VZDRZEVANJU%20SUVI.pdf

[12] Pravilnik o zavarovanju osebnih podatkov (2004). Dostopno 17.2.2014 na: https://www.ip-rs.si/fileadmin/user_upload/doc/Vzorec_pravilnika_za_zavarovanje_OP-1.doc

[13] Priporočila informacijske varnostne politike javne uprave (2010). Dostopno 5.12.2013 na:http://www.mnz.gov.si/fileadmin/mnz.gov.si/pageuploads/JAVNA_UPRAVA/DIES/IVPJU_01.pdf

[14] Proces upravljanja informacijskih tveganj (2010). Dostopno 17.12.2013 na:

http://fl.uni- mb.si/lab_inf/wp-content/uploads/2010/11/konferenca_Skornik_ 2010.pdf

[15] Protivirusni program (2013). Dostopno 15.2.2014 na: http://sl.wikipedia.org/wiki/Protivirusni_program

[16] Smernice za preprečevanje kraje identitete (2012). Dostopno 15.1.2014 na: https://www.ip-rs.si/fileadmin/user_upload/Pdf/brosure/Smernice_kraja_identitete.pdf

[17] Standardi sistemov za upravljanje varovanja informacij (2013). Dostopno 15.12.2013 na http://www.housing.si/sl/Vzorci_varnostnih_politik/

[18] Trampuš M. (2009), Varnostna politika na področju informatike. Dostopno 26.12.2013 na: http://sciget.com/predogled/1595/8ea3dd426017502705a93be95760b31fe991f0e8

[19] Trdina Ž. (2012), Ocena tveganj informacijskega sistema v bolnici Golnik. Dostopno 26.12.2013 na: http://dkum.ukm.si/Dokument.php?id=28096

[20] Upravljanje s tveganji in analiza tveganj (2004). Dostopno 17.12.2013 na: http://www.unp.gov.si/fileadmin/unp.gov.si/pageuploads/notranji_nadzor/Upravljanje_s _tveganji.pdf

[21] Uporaba ISO-standardov skozi informacijsko varnostne politike nadzora dostopa do informacijskega sistema (2012). Dostopno 5.1.2014 na: http://www.fvv.uni-mb.si/DV2012/zbornik/informacijska_varnost/zver_bernik.pdf

[22] Uredba o varstvu dokumentarnega in arhivskega gradiva (2006). Dostopno 18.2.2014 na: http://www.uradni-list.si/1/content?id=74975

[23] Varnostne kopije podatkov (2013). Dostopno 29.12.2013 na: http://www.mat3.si/blog/item/varnostne-kopije-podatkov-backup

[24] Varnostne kopije podatkov v oblakih (2011). Dostopno 4.1.2014 na: http://www.dlib.si/stream/URN:NBN:SI:DOC-YGK0NJZ7/3bfa0b05-5ef9-4fad-9905-f8bd1e576ac8/PDF

[25] Varstvo osebnih podatkov & računalništvo v oblaku (2012). Dostopno 29.12.2013 na: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_rac_v_oblaku.pdf

[26] Vzpostavitev sistema za upravljanje informacijske varnosti v organizaciji (2010). Dostopno 28.12.2013 na: http://www.dlib.si/stream/URN:NBN:SI:DOC-HMQQRLCH /8cb744a1-23e6-4dfe-a25d-5f8c185671dd/PDF

[27] Vzpostavitev sistema za upravljanje informacijske varnosti v organizaciji (2009). Dostopno 5.1.2014 na: http://www.vris.si/Db/vris/content/pdf/Brezascek_ Moskon _Info KomTeh_2009_prispevek.PDF

[28] Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP) (2000). Dostopno 23.1.2014 na: https://www.uradni-list.si/1/content?id=26329

[29] Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA) (2006). Dostopno 22.12.2013 na: http://www.uradni-list.si/1/content?id=72425