UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

UVAJANJE POGOJEV ZA ZAGOTAVLJANJE DELOVANJA POSLOVNEGA INFORMACIJSKEGA SISTEMA

Ljubljana, junij 2003 Boštjan Rihar

IZJAVA

Študent Boštjan Rihar izjavljam, da sem avtor tega magistrskega dela, ki sem ga napisal pod mentorstvom doc. dr. Mojce Indihar Štemberger in skladno s 1.odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovolim objavo magistrskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne _____

Podpis: _____

1 Uvod

1.1 Problem zagotavljanja delovanja poslovnega informacijskega sistema

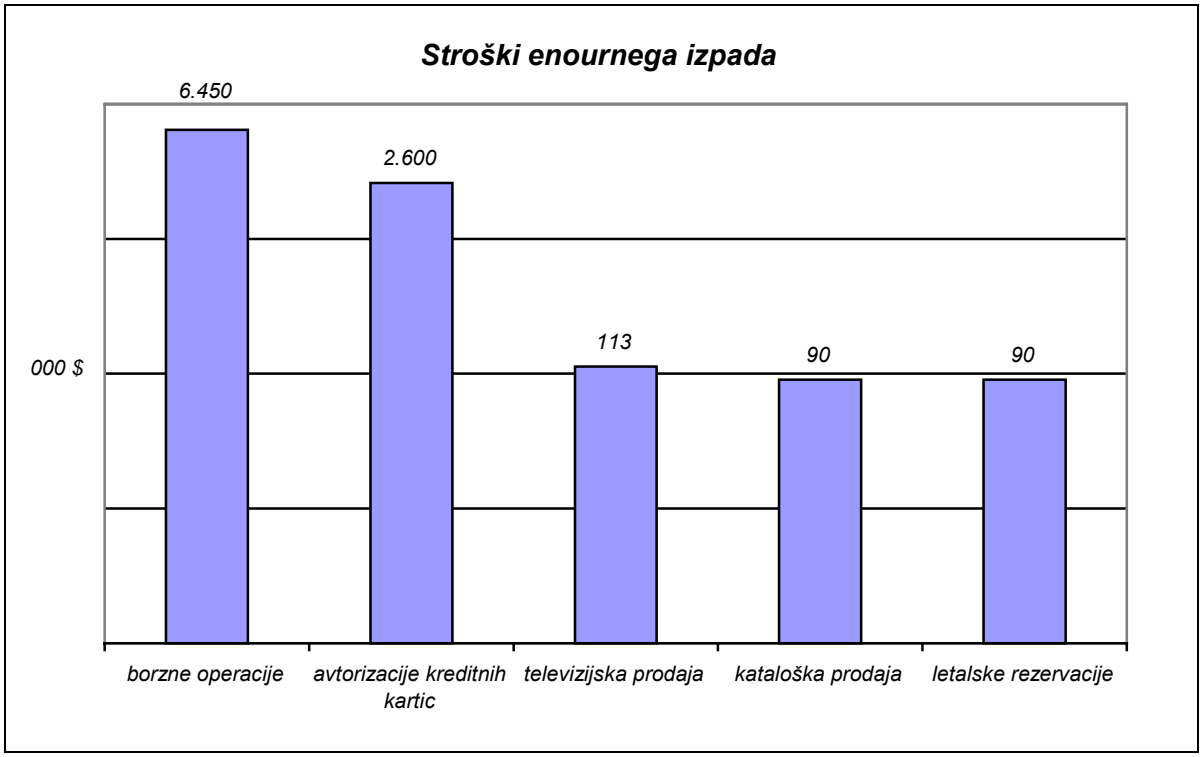
V današnjem času si poslovanja brez podpore učinkovitega poslovnega informacijskega sistema skorajda ne znamo več predstavljati. Čedalje bolj razširjena uporaba novih programskih rešitev, ki so namenjene načrtovanju virov podjetja, upravljanju preskrbovalnih verig ali upravljanju odnosov s strankami, ter čedalje širša uporaba tako imenovanih e-storitev kažeta na to, da bo uspeh poslovanja v prihodnje še bolj odvisen od učinkovite informacijske in telekomunikacijske podpore. Pri tem tako rekoč ni več razlike med pridobitnimi in nepridobitnimi organizacijami, pa tudi razlike med velikimi, srednjimi in malimi podjetji postajajo čedalje manj izrazite.

Hkrati z naraščanjem pomena poslovnih informacijskih sistemov pa narašča tudi obseg potencialne škode, ki jo utrpijo organizacije ob prekinitvi njihovega delovanja. Vsak izpad informacijske podpore hkrati pomeni tudi izpad dohodka, v nekaterih primerih, če izpad traja predolgo, ali če se nekateri ključni podatki trajno izgubijo, pa tudi grožnjo za obstoj same organizacije. Prav zato so na nekaterih področjih, na primer v bančništvu, v vladnih organizacijah, na telekomunikacijah, v transportu ipd., poslovni informacijski sistemi obravnavani kot kritična infrastruktura (Verton, 2002 b).

Gartnerjeva raziskava je pokazala, da kar dve petini podjetij, ki so doživela nesrečo večjih razsežnosti, preneha poslovanje bodisi takoj bodisi, zaradi neuspešnega okrevanja, v naslednjih nekaj letih (Wheatman, 2001). Razlogi za to so različni, od posledic padca zaupanja strank v poslovanje organizacije, do prevelike cene ali celo nezmožnosti sistema za okrevanje. Vendar pa je ista raziskava pokazala tudi, da se možnost preživetja organizacije bistveno izboljša, če ima organizacija pripravljen načrt zagotavljanja nadaljevanja poslovanja. Kun in Furlonger navajata primer uspešnega okrevanja po izpadu informacijske podpore zaradi posledic terorističnega napada na World Trade center 11. septembra 2001 za dve pomembni organizaciji, New York Stock Exchange in American Stock Exchange (Kun, Furlonger, 2002).

Seveda pa niso problematični le katastrofalni izpadi. Zaradi vse hujše globalne konkurence in zaradi potrebe po vedno hitrejšem reagiranju na tržno dogajanje lahko tudi krajši in manj obsežni izpadi pomenijo hudo grožnjo za obstanek podjetja. Če je še pred desetletjem ali dvema veljalo, da večina podjetij lahko zdrži brez hujših posledic tudi do šestdnevni izpad informacijske podpore (Toigo, 2000, str. 5), se je danes ta meja močno znižala – v nekaterih panogah že na nekaj ur ali celo manj.

Fibre Channel Industry Association je zbrala podatke o stroških enournega izpada delovanja poslovnega informacijskega sistema v različnih organizacijah v ZDA. Podatki za nekatera najbolj zanimiva poslovna področja so prikazani na sliki 1.

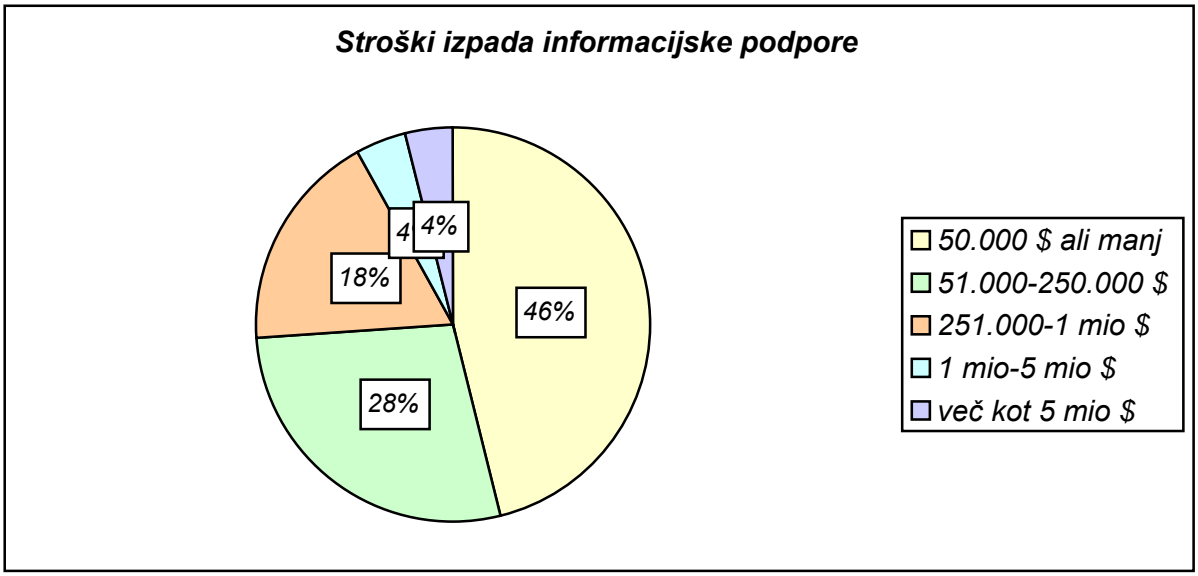


Slika 1: Stroški enournega izpada na nekaterih poslovnih področjih v ZDA za leto 1995 (Vir: The Fibre Channel Industry Association, www.fibrechannel.com)

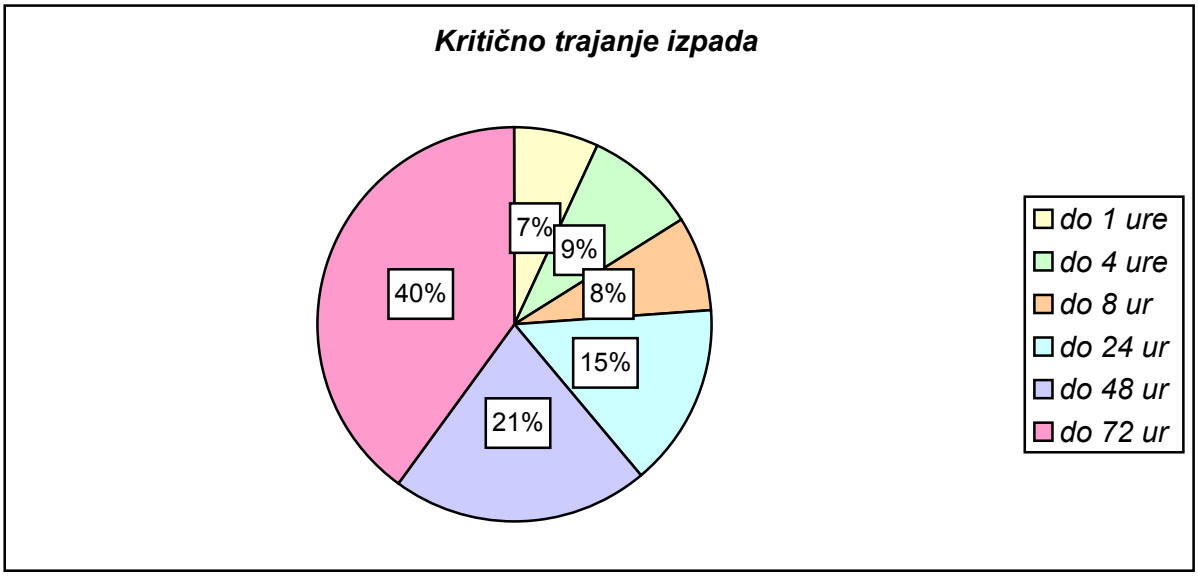
Še bolj zanimivi so podatki, ki jih je leta 2001 zbrala Eagle Rock Alliance v svoji spletni anketi na temo posledic izpada informacijske podpore. Anketa je bila izvedena med ameriškimi organizacijami različnih velikosti z letnimi dohodki od nekaj milijonov do več kakor pet milijard dolarjev. Na sliki 2 je prikazana razvrstitev organizacij glede na neposredne stroške enournega informacijskega mrka. Poleg neposrednih stroškov so respondenti ocenjevali tudi druge, nemerljive posledice izpada in pri tem na prvih dveh mestih navajali upad zaupanja pri strankah in izgubo konkurenčnosti. Zanimivi so tudi odgovori na vprašanje, kako dolg izpad bi po mnenju respondentov lahko že ogrozil obstoj njihove organizacije. Razvrstitev organizacij glede na ocenjeno kritično trajanje izpada je prikazana na sliki 3.

Na nekaterih poslovnih področjih se je pokazalo, da ima izpad informacijske podpore lahko tako velike negativne posledice, da je bilo treba ustrezno preventivno delovanje zagotoviti tudi z zakonsko regulativo. Ta potreba se je najprej pokazala v bančništvu, pozneje pa še v drugih finančnih institucijah, v državni upravi, na področju telekomunikacij in drugod. V

ZDA je bil že leta 1983 sprejet prvi zakon, ki je bankam predpisoval, da morajo izdelati in vzdrževati ustrezne okrevalne načrte za ponovno vzpostavitev poslovanja v primeru izpada informacijske podpore, v naslednjih letih pa je bila tam sprejeta še vrsta predpisov in zakonov tudi za druga poslovna področja (Toigo, 2000, str. 12, 13).



Slika 2: Deleži organizacij glede na stroške enournega izpada v ZDA za leto 2001 (Vir: Eagle Rock Alliance, www.contingencyplanningresearch.com)



Slika 3: Kritično trajanje izpada (Vir: Eagle Rock Alliance, ibid.)

Tudi v Sloveniji so na tem področju orali ledino v bančništvu. Banka Slovenije je v tako s Sklepom o določitvi pogojev, ki jih morajo izpolnjevati banke za opravljanje bančnih storitev, ki je bil objavljen v Uradnem listu št. 52/2000 13. junija 2000, postavila pogoj, da so vse banke in hranilnice pri svojem poslovanju dolžne upoštevati slovenski standard PSIST BS 7799 (zdaj standard ISO 17799). Ta standard predpisuje postopke, ki jih mora organizacija izpeljati, da prepreči prekinitve poslovnih dejavnosti in zaščiti kritične poslovne procese pred učinki večjih napak in nesreč.

Zgledu Banke Slovenije je sledil Center vlade za informatiko, ki je pripravil Priporočila za pripravo informacijske varnostne politike za organe javne uprave, ki jih je s sklepom potrdila vlada RS na svoji seji 3. oktobra 2002. V sicer neobveznem sklepu vlada poziva organe javne uprave, da začnejo čim prej zagotavljati in vzdrževati ustrezno informacijsko varnost, in sicer z analizo tveganja, z ukrepi za zmanjšanje tveganja ter z uvajanjem pravil za zagotavljanje varnosti, in da naj si pri teh postopkih pomagajo s priporočili, ki jih je pripravil Center vlade za informatiko. V priporočilih, ki so narejena na podlagi standarda ISO 17799, so našteti različni ukrepi in postopki, ki jih v javni upravi lahko izpeljejo za izboljšanje informacijske varnosti.

Za druga poslovna področja v Sloveniji za zdaj ni tako obvezujočih predpisov, vendar pa velja, da morajo organizacije, ki želijo pri svojem delovanju upoštevati določila standarda ISO 9002, upoštevati tudi določila o zagotavljanju delovanja poslovnega informacijskega sistema.

Kljub temu pa je zanimivo, da se zavest o tem, da je treba uvajati rešitve za zagotavljanje delovanja poslovnega informacijskega sistema, širi presenetljivo počasi. Anketa, ki jo je novembra 2001 izvedlo podjetje Ernst & Young International na vzorcu 459 srednjih in večjih organizacij po vsem svetu je pokazala, da ima le 53 odstotkov teh organizacij izdelan načrt zagotavljanja nadaljevanja poslovanja v primeru večje nesreče (Verton, 2002 a). Ista anketa pa je tudi pokazala, da slaba desetina od tistih organizacij, ki ima izdelan tak načrt, tega nikoli ni zares testirala.

Stanje pa je še precej slabše v manjših podjetjih. Raziskava, ki jo je v letih 2000 in 2001 izvedla Compass America po ameriških organizacijah srednje velikosti, je pokazala, da ima le ena četrtina teh organizacij izdelan okrevalni načrt, od katerih pa jih ena tretjina svojega načrta ni nikoli preizkusila (Boroski, 2002). Na podlagi podatkov te raziskave je bilo ocenjeno, da lahko le približno 15 odstotkov tovrstnih organizacij ponovno vzpostavi več kot tretjino svojih poslovnih aplikacij, da pa jih manj kot štiri odstotke lahko ponovno vzpostavi svoje aplikacije v enem dnevu ali manj.

Gartner ocenjuje, da ima z izjemo finančnih institucij ažurne in učinkovite načrte zagotavljanja nadaljevanja poslovanja le 10 do 15 odstotkov velikih organizacij in da je stanje pri srednjih in malih organizacijah še slabše (Scott, Gassman, 2001).

Tudi študija revizijske družbe KPMG je pokazala, da je kakovost načrtov za zagotavljanje poslovanja, ki jih imajo organizacije izdelane, relativno slaba. Po tej študiji lahko svoje zastavljene cilje doseže le slaba polovica tovrstnih načrtov. Poglavitna razloga za to sta predvsem razdrobljenost teh načrtov po posameznih poslovnih enotah in neažurnost (Noakes-Fry, Diamond, 2001).

Ocene o tem, koliko sredstev namenjajo organizacije zagotavljanju poslovanja, se zelo razlikujejo. Gartner opaža, da v organizacijah ne vedo prav natančno, koliko potrošijo na tem področju in da se različne ocene gibljejo od 2 do 15 odstotkov celotnih izdatkov za informatiko (Witty et al., 2001). IDC po drugi strani v svojih analizah ocenjuje, da na svetovni ravni organizacije namenjajo okrevalnim načrtom in zagotavljanju nadaljevanja poslovanja v povprečju okrog pol odstotka svojih izdatkov za informacijsko tehnologijo (Everett, 2002).

Po ocenah IDC so leta 2001 znašali skupni izdatki za to področje v Evropi nekaj manj kakor milijardo dolarjev (Everett, 2002). Anketa Network World, objavljena maja letos, je pokazala, da na območju ZDA ti stroški za velike organizacije znašajo v povprečju 3,9 milijona dolarjev, kar je približno 200.000 dolarjev več, kakor leto prej (Hoffman, 2002). Anketa Computerworld je pokazala, da je približno polovica organizacij v ZDA po terorističnem napadu 11. septembra 2001 sprejela ukrepe za izboljšanje stopnje zagotavljanja poslovanja, da pa je le slaba tretjina od njih v ta namen predvidela dodatna sredstva, drugi pa so le prerazporedili sredstva, ki so bila že načrtovana za razvoj informacijske tehnologije (Hall, 2002).

Kaj pa v Sloveniji? V naši državi doslej še ni bila narejena še nobena raziskava, ki bi dala vsaj približen odgovor na to, kako to problematiko rešujejo naše organizacije. Glede na neformalne informacije, do katerih je bilo mogoče priti v pogovorih s skrbniki informacijskih sistemov v nekaterih večjih organizacijah in s prodajnimi predstavniki podjetij informacijske in telekomunikacijske tehnologije, pa je mogoče sklepati, da je stanje na tem področju zelo slabo. Z izjemo bančnih institucij, ki so za zagotavljanje delovanja poslovnega informacijskega sistema dolžne skrbeti po sklepu Banke Slovenije, v drugih organizacijah, tako zasebnih kot javnih, v tej smeri do zdaj niso naredili prav veliko ali celo ničesar. To za organe javne uprave v prej omenjenem sklepu ugotavlja tudi vlada RS, ki meni, da imajo različni organi uveljavljene dokaj različne standarde informacijske varnosti, ki pa v nobenem primeru ne rešujejo tega problema celovito in sistemsko.

V pomembnejših bančnih institucijah jim je, kolikor so mi bili podatki dostopni, uspelo zagotoviti le minimalne zahteve navedenega sklepa, kar pomeni, da imajo zagotovljeno kopiranje podatkov na oddaljeno lokacijo. Resnejših strategij za zagotavljanje delovanja informacijskega sistema v primeru večje nesreče za zdaj nimajo, ali pa jih šele načrtujejo. Razlogi za to stanje so klasični: previsoka cena, ki je ni mogoče poslovno upravičiti ali

izkoristiti kot konkurenčno prednost, tehnološka zahtevnost zaradi močne razdrobljenosti informacijskih sistemov, majhna verjetnost takih dogodkov in to, da tudi konkurenca nima podobnih rešitev.

1.2 Reševanje problema

V državah z visoko razvito informacijsko tehnologijo se je način zagotavljanja delovanja poslovnih informacijskih sistemov v zadnjih desetih letih precej spremenil. Vzrok za to gre iskati v precejšnjih tehnoloških spremembah v informatiki in telekomunikacijah, v novih načinih uporabe informacijske tehnologije in v čedalje bolj izraziti potrebi po neprekinjenem 24-urnem delovanju poslovnih informacijskih sistemov.

Do pred približno desetimi leti se je razmišljalo predvsem o okrevanju po morebitni nesreči (*disaster recovery*). Okvir reševanja problema je bil omejen na sam informacijski sistem, ki je bil tipično centraliziran. Problema so se lotevali tako, da so nekako skušali zavarovati kritične podatke pred uničenjem, tako da bi jih bilo mogoče ob morebitni nesreči ponovno deloma ali v celoti vzpostavili na kaki drugi lokaciji. Ker so bili sistemi centralizirani, jih je bilo relativno preprosto »klonirati«, prav tako pa ni bilo težav s kopiranjem pomembnih podatkov in aplikacij. Kljub temu je bil pričakovani čas ponovne vzpostavitve sistema tri dni ali več, kar pa je bilo takrat povsem sprejemljivo. Organizacije, večinoma s finančnega področja, so se problema lotevale predvsem zaradi zakonskih obveznosti in strahu pred trajno izgubo podatkov.

V zadnjem desetletju pa je zaradi širitve informacijske podpore na vedno širši segment poslovanja ta okvir postajal preozek. Zaradi vsesplošne razširjenosti distribuiranih informacijskih rešitev, uvajanja integriranih programskih rešitev, ki so namenjene upravljanju poslovnih virov, vse večjega uveljavljanja e-poslovanja, zunanjega izvajanja del idr., ko je postalo jasno, da je možnosti za preproste tehnične rešitve čedalje manj, se je pozornost začela obračati k zagotavljanju izvajanja delovnih procesov oziroma zagotavljanju nadaljevanja poslovanja (*business continuity*). S tem pa se je začela tudi odgovornost za uvajanje rešitev seliti s tehničnega vse bolj na organizacijsko oziroma poslovno področje (Scott, Witty, 2001, Witty, 2001 a, Younker, 2001).

Prav zaradi hitrega spreminjanja okvira problematike zagotavljanja delovanja poslovnih informacijskih sistemov v zadnjih letih vlada na tem področju precejšnja pojmovna in metodološka različnost. Razni avtorji si okvir in glavno težišče reševanja problematike razlagajo različno, odvisno od tega, ali izhajajo bolj s poslovnega, ali bolj z informacijskega področja. Zaradi naglih sprememb ni niti splošno sprejetih tehničnih standardov, pa tudi terminologija se med različnimi avtorji in ponudniki storitev s tega področja še precej razlikuje (glej na primer intervju BCP Comes of Age, ki ga je naredil Information Security Magazine s tremi strokovnjaki s tega področja).

Kljub temu pa je mogoče na podlagi gibanj zadnjih let iz različnih metodologij izluščiti nekatere skupne lastnosti, ki naj pokažejo točko konvergence, h kateri naj bi metodologije vodile. Poglavitna predpostavka je, da je poslovni informacijski sistem v sodobni organizaciji bistveni povezovalni element, brez katerega poslovanje ni več mogoče. Poslovni informacijski sistemi že tradicionalno skrbijo za pretok podatkov, ki se izmenjujejo v organizaciji, v zadnjih letih pa postajajo vse bolj nepogrešljivi tudi pri zagotavljanju izmenjave podatkov med organizacijo in njeno okolico (drugimi organizacijami in posamezniki). To seveda ne velja enako za vsa poslovna področja in tudi ne za vse organizacije, vendar pa so težnje nedvoumne.

Iz te predpostavke izhaja temeljno izhodišče tega dela, da je treba pripravo organizacije na nepredvidene dogodke, ki lahko ogrozijo njeno poslovanje, začeti pri načrtu zagotavljanja delovanja njenega poslovnega informacijskega sistema. Prvi razlog za to je v že prej navedeni čedalje tesnejši povezanosti večine funkcij poslovnega sistema skozi poslovni informacijski sistem, zaradi česar lahko z opazovanjem delovanja posameznih njegovih delov opazujemo tudi delovanje posameznih funkcijskih enot poslovnega sistema. Drugi razlog pa je v tem, da poslovni informacijski in telekomunikacijski sistem zaradi svoje fizične razprostranjenosti, tehnološke zapletenosti in čedalje tesnejše navezave z okoljem ter s tem čedalje večje odprtosti pomeni enega najbolj ranljivih delov poslovnega sistema.

Spremembe, ki se pri zagotavljanju delovanja poslovnih informacijskih sistemov dogajajo v zadnjih letih, se v literaturi odražajo v precejšnjem številu različnih metodologij oz. načinov, na katere se je mogoče lotiti te problematike. Iz različnih metodologij bi lahko izluščili nekatere skupne lastnosti in jih opisali z naslednjimi koraki, ki bodo ločeno obdelani tudi v pričujočem magistrskem delu.

- ***Analiza tveganja in analiza vpliva na poslovanje***. Obe analizi sta temelj vsakega načrtovanja zagotavljanja delovanja informacijskega sistema v organizaciji. V okviru prve analize je treba poiskati dejavnike tveganja, opredeliti nevarnosti, ki pretijo delovanju informacijskega sistema, in točke v sistemu, ki bi lahko bile prizadete. Z drugo analizo je treba ovrednotiti neposredno in posredno škodo, ki bi jo povzročili posamezni potencialni izpadi, evidentirani v okviru prve analize. Na podlagi te analize se določijo tudi temeljni parametri, ki bodo upoštevani pri izdelavi okrevalnega načrta.

- ***Preventivno delovanje***. Namen preventivnega delovanja je z ustreznimi akcijami izločiti oziroma bistveno zmanjšati možnost, da bi nepričakovani dogodek prizadel poslovni informacijski sistem, ali pa vsaj omiliti posledice, če se takemu dogodku ne da izogniti. Večinoma gre pri tem za fizično zaščito prostorov in strojne opreme, logično zaščito programske opreme in omrežij ter nadzor zaposlenih.

- ***Izdelava okrevalnega načrta ali načrta nadaljevanja poslovanja***. V tem delu se metodologije med sabo najbolj razhajajo, predvsem zaradi različnega pojmovanja pomena informatike za poslovanje organizacije in s tem tudi okvira, ki naj ga načrt obsega. Ta obseg se od organizacije do organizacije spreminja, vsekakor pa mora pred izdelavo načrta v organizaciji glede tega obstajati jasen konsenz. Na splošno pa mora načrt vsebovati:

    - postopke za restavriranje podatkov in programske opreme,
    - postopke za restavriranje strojne opreme,
    - postopke za vzpostavitev telekomunikacijskih povezav,
    - postopke za vzpostavitev poslovanja.

- ***Testiranje in vzdrževanje***. Redno testiranje in prilagajanje načrta tehničnim in organizacijskim spremembam je nujno, sicer načrt ostane mrtva črka na papirju in prav kmalu postane neuporaben. Pomembno je tudi, da se v organizaciji na vseh ravneh oblikuje zavestna in trajna skrb za ohranjanje dosežene ravni zagotavljanja delovanja poslovnega informacijskega sistema.

1.3 Namen in cilja magistrskega dela

Ne glede na to, da se je v zadnjih letih, še posebno v zadnjem letu, pozornost organizacij do problema zagotavljanja delovanja poslovnega informacijskega in telekomunikacijskega sistema vendarle povečala, je iz navedenih podatkov razvidno, da je pomen, ki ga organizacije pripisujejo tej problematiki, še vedno relativno majhen. To dejstvo je v Sloveniji še posebej očitno, kar se kaže tudi v tem, da v slovenščini ni zaslediti dela, ki bi se ukvarjalo s tem področjem. Namen magistrskega dela je zato predvsem dati tej problematiki ustrezen poudarek in jo s tem priklicati v zavest tistih, ki so odgovorni za razvoj informatike v svojih organizacijah.

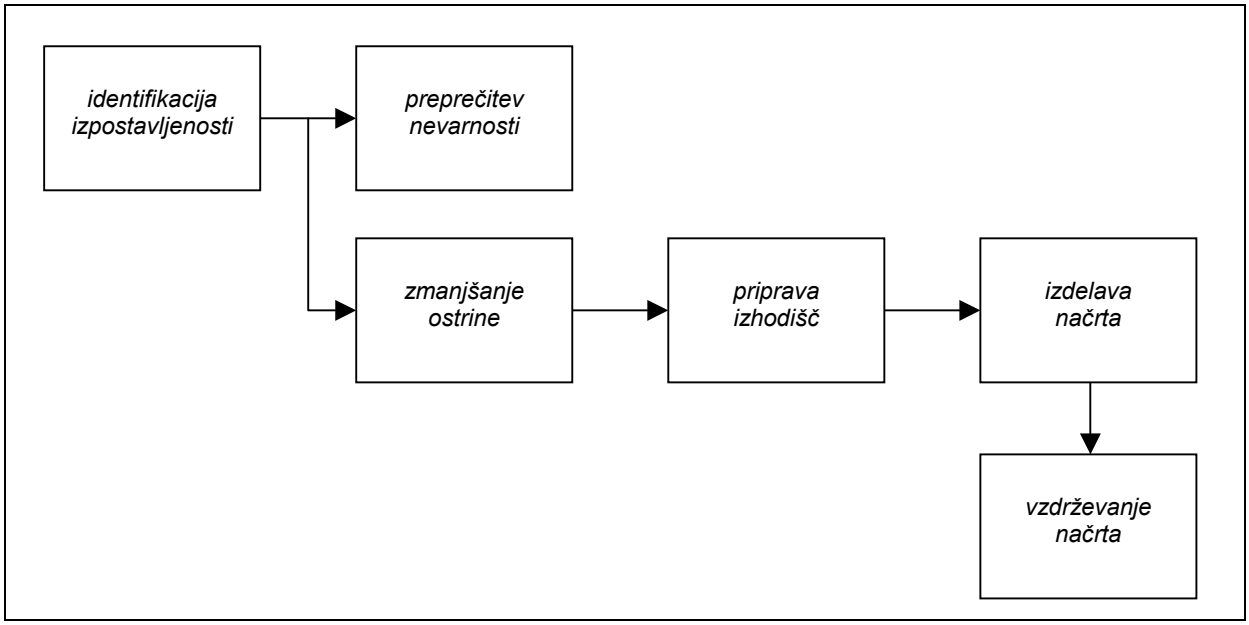
Cilja magistrskega dela sta:

1. Iz različnih dostopnih metodologij zagotavljanja delovanja informacijskega sistema, ki jih je mogoče zaslediti v literaturi, izluščiti najpomembnejše značilnosti in jih povezati v smiselno celoto, ki bi lahko služila kot referenca pri reševanju tega problema.

2. Prikazati konkretni primer združitve splošnih metodoloških spoznanj in praktičnih izkušenj pri reševanju tega problema v slovenski policiji.

2 Analiza tveganja

Postopek uvajanja pogojev za zagotavljanje delovanja poslovnega informacijskega sistema na zelo preprost način prikazuje procesni diagram na sliki 4.



Slika 4: Zagotavljanje delovanja poslovnega informacijskega sistema
(Vir: Toigo, 2000, str. 57)

Analiza tveganja (*Risk Analysis*), v literaturi tudi upravljanje tveganja (*Risk Management*) ali analiza vpliva na poslovanje (*Business Impact Analysis*), pomeni prvo in najpomembnejšo fazo pri uvajanju pogojev za zagotavljanje delovanja poslovnega informacijskega sistema organizacije in s tem njenega poslovanja. Namen te faze je razumeti nevarnosti, katerim je delovanje informacijskega sistema in s tem poslovanje organizacije izpostavljeno, saj je le tako mogoče izbrati najbolj ustrezno metodo zagotavljanja poslovanja in pridobiti za to nalogo ustrezno podporo vodstva organizacije. Cilj analize tveganja je preprost: poiskati povezave med poslovanjem organizacije in njegovo izpostavljenostjo različnim tveganjem, ki mu pretijo. Vendar pa je treba za dosego tega cilja izpeljati zelo širok razpon različnih dejavnosti in postopkov.

2.1 Postopki in pomen analize tveganja

V tej fazi so zaradi različnega obsega opazovanja in različnih poudarkov razlike med metodologijami precejšnje, poleg tega se zaradi pojavljanja novih tehnologij in novih oblik

groženj v podrobnostih stalno spreminjajo. Toigo opredeljuje naslednje splošne dejavnosti, ki jih je treba izpeljati v tej fazi (Toigo, 2000, str 38, 39):

- identificirati poslovne procese v organizaciji in informacijske ter telekomunikacijske komponente, ki te procese podpirajo,
- ugotoviti ali izmeriti vpliv nenačrtovane prekinitve vsakega poslovnega procesa,
- izdelati seznam možnih groženj, ki pretijo poslovnim procesom, ter jih razvrstiti glede na verjetnost pojavljanja in obseg potencialnega vpliva.

Levitt to fazo imenuje upravljanje tveganja in jo opredeljuje s štirimi koraki, ki pravzaprav vsebujejo celoten koncept zagotavljanja poslovanja (Levitt, 1999, str 160):

- identifikacija groženj,
- ugotavljanje verjetnosti pojavljanja nepredvidenih dogodkov in njihovega vpliva na poslovanje,
- zmanjševanje tveganja,
- vzpostavitev pogojev za nadaljnje poslovanje.

Kreizman in Mingay v okviru te faze opredelita naslednje štiri skupine dejavnosti (Kreizman, Mingay, 2001):

- razviti scenarije možnih nepredvidenih dogodkov,
- identificirati poslovne procese,
- ugotoviti finančne in druge vplive definiranih scenarijev na poslovne procese,
- opredeliti cilje okrevalne strategije.

Hiles to fazo na kratko opredeli kot identificiranje vplivov na organizacijo ob nepredvidenih dogodkih, katere cilji naj bi bili naslednji (Hiles, 2002):

- identifikacija finančnih in drugih stroškov,
- določitev časa, potrebnega za ponovno vzpostavitev poslovanja,
- opredelitev ključnih objektov, ki so potrebni za nadaljevanje poslovanja,
- ocena stroškov, potrebnih za nadaljevanje poslovanja,
- dati problematiki ustrezen pomen pri poslovodstvu in zaposlenih.

Kljub precejšnjim razlikam v podrobnostih si je večina avtorjev enotnih glede pomena, ki ga ima ta faza v procesu zagotavljanja delovanja poslovnega informacijskega sistema. Izsledki te

faze najpomembneje vplivajo na način in obseg reševanja te problematike v organizaciji, ne glede na to, ali je višji menedžment, zaradi zakonskih obveznosti ali drugih razlogov, že sprejel načelno odločitev o izvedbi programa uvajanja rešitev, ali pa je morebitni sprejem take odločitve odvisen od izsledkov te analize. V drugem primeru imajo prav ugotovitve analize tveganja ključni vpliv za doseganje podpore v vodstvu organizacije in s tem na odločitev o uvajanju pogojev za zagotavljanje poslovanja. Zato mora biti ta faza izvedena izjemno skrbno in racionalno, a brez nepotrebnega pretiravanja.

Analizo tveganja sestavljata dva dela: zbiranje podatkov in njihova analiza. V okviru prvega dela je treba zbrati podatke o poslovanju, informacijski podpori in varnostni situaciji v organizaciji ter podatke o grožnjah, ki pretijo delovanju informacijskega sistema. Količina in obseg podatkov, ki jih je treba zbrati, je odvisna predvsem od obsega, ki ga želi organizacija zajeti s programom uvajanja pogojev za nadaljevanje poslovanja.

2.1.1 Identifikacija strank

Pred začetkom zbiranja podatkov je treba identificirati najpomembnejše stranke, ki so zainteresirane, da organizacija posluje v okviru pričakovanj. Malik navaja naslednje tri vrste strank, katerih pričakovanja do organizacije se med sabo razlikujejo (Malik, 2001):

- poslovni partnerji, ki želijo nemoteno poslovati z organizacijo,
- zaposleni, ki jih zanima njihova usoda v zvezi z zaposlitvijo in varnostjo v organizaciji,
- investitorji, ki potrebujejo zagotovila, da so njihove investicije v organizaciji varne.

Noakes-Fry in Diamond k tem trem dodajata še zakonodajalce, ki terjajo, da je zakonskim zahtevam ne glede na okoliščine zadoščeno, in zavarovalnice, ki pričakujejo, da se vodi ustrezna skrb za zavarovane entitete (Noakes-Fry, Diamond, 2001).

2.1.2 Zbiranje podatkov

Ko so najpomembnejše stranke identificirane, je treba zbrati naslednje kategorije podatkov:

- ***podatke o poslovnih procesih v organizaciji:***
  - pomen posameznih poslovnih procesov,
  - medsebojna odvisnost poslovnih procesov,
  - odvisnost od zunanjih partnerjev;
- ***zakonske in pogodbene zahteve:***
  - zakonodaja,

    - pogodbe z zunanjimi partnerji;
- ***podatke o informacijski podpori poslovnih procesov:***
    - aplikacije,
    - podatki,
    - strojna oprema,
    - povezave z okoljem,
    - zunanji ponudniki informacijskih storitev;
- ***podatke o infrastrukturi:***
    - zgradbe,
    - telekomunikacijske povezave,
    - energetska oskrba,
    - prometne povezave;
- ***podatke o zaposlenih:***
    - ključne osebe,
    - možnost dostopa do različnih lokacij;
- ***varnostne podatke:***
    - varnostni elementi infrastrukture,
    - zaščita informacijskega sistema,
    - varnostni standardi v organizaciji;
- ***podatke o nevarnostih:***
    - zunanje nevarnosti,
    - notranje nevarnosti.

Večino potrebnih podatkov je mogoče pridobiti v organizaciji sami, in sicer od pristojnih oddelkov ali služb. Podatke o poslovnih procesih je najbolje zbrati v posameznih oddelkih organizacije z uporabo vprašalnikov (primer glej Fulmer, 2000, str. 51–57) in z osebnimi pogovori. Pri tem je treba biti ustrezno selektiven, saj se je treba osredotočiti le na tiste poslovne procese, ki oskrbujejo pomembne stranke, čeprav bo dokončno razvrstitev po pomembnosti pozneje dala šele analiza. Splošnejši pregled medsebojne odvisnosti poslovnih procesov pozna vodstvo organizacije, delno pa tudi služba za informatiko, ki je hkrati glavni vir podatkov glede informacijske podpore poslovnih procesov in zaščite informacijskega sistema.

Podatke o telekomunikacijski in energetski oskrbi je treba pridobiti od zunanjih ponudnikov. V Sloveniji je s pridobivanjem teh informacij precej težav, saj jih ponudniki zelo neradi posredujejo. Na področju telekomunikacij je trenutno glavni ponudnik Telekom Slovenije, ki edini omogoča povezavo do vseh točk v Sloveniji, vendar načelno ne oddaja polne zmogljivosti optičnega vlakna. Drugi ponudniki, ki so s ponudbo omejeni le na območje svoje infrastrukture, kot na primer Elektro-Slovenija, Slovenske železnice, DARS ali Telemach, poleg najema zmogljivosti nudijo tudi najem optičnih vlaken. Za zdaj ima le Telekom na nekaterih delih svojega omrežja predvidene alternativne poti v primeru prekinitve primarne

komunikacijske povezave, medtem ko drugi ponudniki te možnosti nimajo. Oskrba z električno energijo je v domeni lokalnih elektrodistribucijskih ponudnikov, ki na splošno nimajo na voljo rezervnih kapacitet v primeru prekinitve povezav ali izpada transformatorskih postaj. V omejenem obsegu pa je mogoče izpad električne oskrbe relativno enostavno nadomestiti z napravami za neprekinjeno napajanje in električnimi agregati.

2.1.3 Identifikacija nevarnosti

Nevarnosti, ki pretijo delovanju informacijskega sistema in poslovanju organizacije so zelo različne, tako po načinu nastanka kot po obsegu in verjetnosti pojavljanja. V literaturi je mogoče najti vrsto različnih seznamov in razvrstitev nevarnosti. Tate in drugi denimo navajajo listo več kakor 70 različnih nevarnosti, ki pretijo delovanju informacijskega sistema (Tate et al., 2002, str. 42). Mayer nevarnosti deli v tri skupine, in sicer (Mayer, 1999, str. 33, 34):

- ***naravne:***
  - poplave,
  - potresi,
  - viharji,
  - ogenj;
- ***okoljske:***
  - letalske nesreče,
  - eksplozije,
  - kontaminacije,
  - prekinitev telekomunikacijskih povezav;
- ***namerne:***
  - požigi,
  - sabotaže,
  - vandalizem;

Fulmer, katerega izhodišče je, da je treba upoštevati le najpogostejše nevarnosti, navaja naslednjo razvrstitev (Fulmer, 2000, str. 38):

- požari,
- nesreče z nevarnimi materiali,
- poplave in izliv vode,
- viharji,
- potresi,
- tehnični izpadi.

Pisanje zelo podrobnega seznama možnih nevarnosti je seveda nesmiselno in jalovo početje, saj spisek nikoli ne more biti popoln. Vsekakor pa je treba imeti pri analiziranju tveganja pred očmi temeljni pregled možnih izpostavljenosti. Seznam potencialnih nevarnosti je odvisen od države in lokacije (ali lokacij), na kateri se organizacija nahaja, od vrste dejavnosti in načina organiziranosti, zato ni mogoče uporabljati splošnega, temveč si mora vsaka organizacija sestaviti svoj posebni seznam nevarnosti in groženj.

Nevarnosti je mogoče razdeliti tudi glede na izvor, to je na notranje in zunanje. Taka razdelitev je nekoliko preglednejša, saj je preprečevanje nevarnosti v vsakem primeru različno, poleg tega so notranje nevarnosti navadno precej bolj specifične za posamezno organizacijo, kakor zunanje. Zunanje nevarnosti, na katere je mogoče računati v Sloveniji, so naslednje:

- potres,
- poplava (tudi dvig podtalnice),
- požar,
- izpad telekomunikacijskih povezav,
- izpad napajanja,
- računalniški vdor/virus,
- nevarne snovi v bližnji okolici,
- vlom, tatvina.

Najpogostejše notranje nevarnosti so:

- požar, eksplozija,
- nevarne snovi,
- poškodbe prostorov/napeljav,
- okvara strojne opreme,
- napaka v programski opremi,
- sabotaža,
- nenamerna napaka zaposlenih.

Spisek notranjih nevarnosti je le okviren, natančnejši seznam je mogoče sestaviti z uporabo statističnih podatkov o tovrstnem dogajanju v organizaciji ali v podobnih organizacijah v preteklosti. Ocene možnega pojavljanja zunanjih nevarnosti se nahajajo v javnih statističnih bazah, v javnih občilih in strokovni literaturi, v internetu ali pri pristojnih službah. Tudi seznam zunanjih nevarnosti ni dokončen, saj se vztrajno pojavljajo nove vrste groženj, ki jih je treba upoštevati. Tako se je nevarnost vdora v informacijski sistem in napada z

računalniškimi virusi (trojanskimi konji, črvi) resneje pojavila šele v zadnjih letih z razširjanjem uporabe interneta, pojavlja se možnost terorističnih napadov itd.

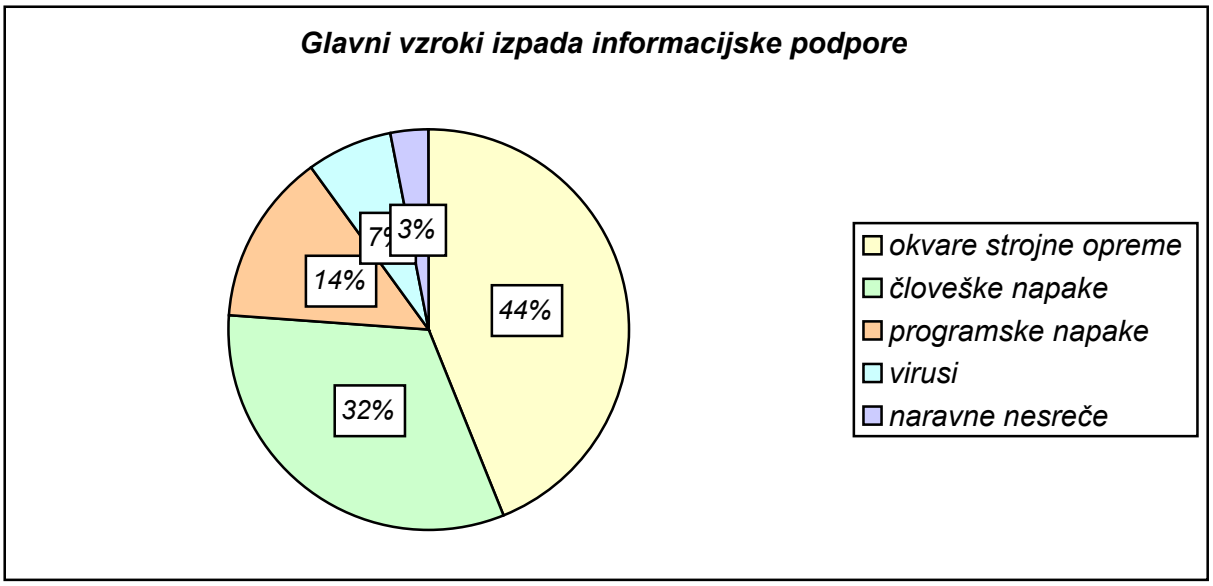
2.1.4 Načrtovani izpadi

Vendar pa nepričakovani dogodki niso edini vzrok za izpad informacijske podpore. Zelo pomemben in večkrat prezrt razlog za izpad so tudi zaustavitve zaradi rednega vzdrževanja, obnavljanja, razširitve ali prenove strojnega oziroma programskega dela informacijskega sistema. Čedalje večji del tovrstnih posegov je sicer mogoče opraviti na delujočem sistemu, vendar se prav vsem zaustavitvam nikoli ne bo mogoče izogniti.

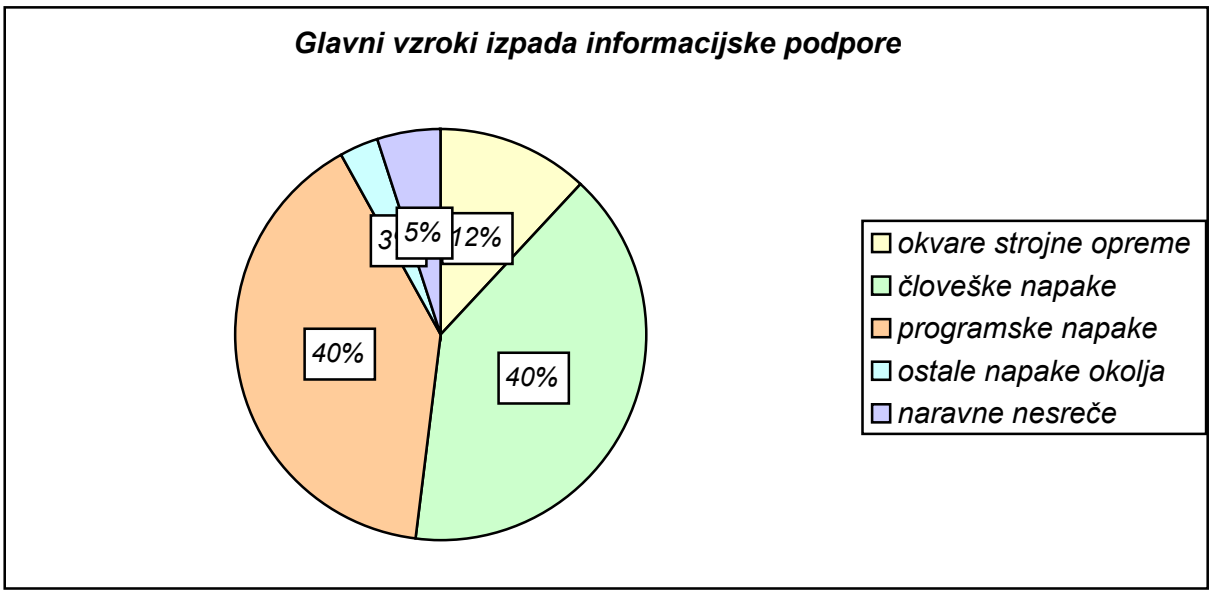
Ker vzdrževalni posegi navadno povzročijo relativno dolge izpade, ki lahko trajajo tudi 24 ur ali dlje, je treba v analizi tveganja upoštevati tudi te, čeprav so ti izpadi načrtovani in jih v tem pogledu ni mogoče opredeliti kot dejavnike tveganja. Po eni strani vpliva na obseg tovrstnih posegov sama izbira tehnološke platforme in strukture informacijskega sistema, kar je treba upoštevati že pri načrtovanju njegovega razvoja ali prenove. Poleg tega pa je treba pri uvajanju pogojev za zagotavljanje delovanja informacijskega sistema iskati take rešitve, ki bodo uspešno nadomestile informacijsko podporo tudi ob načrtovanih izpadih.

2.1.5 Najpogostejši vzroki izpadov

Kateri so, statistično gledano, najpogostejši vzroki izpada informacijske podpore? Zanimivo je, da so naravne nesreče, ki lahko povzročijo največjo materialno škodo in so navadno glavni razlog za odločitev organizacije za uvajanje pogojev za zagotavljanje delovanja informacijskega sistema, vzrok za relativno majhen del izpadov informacijske podpore. Podatki različnih raziskav se sicer zaradi razlik v klasifikaciji in pojmovanju vzrokov med sabo delno razlikujejo, kljub temu pa vendarle jasno pokažejo, da daleč največji delež izpadov informacijske podpore nastane zaradi napak zaposlenih, okvar strojne opreme in okvar ali slabega delovanja programske opreme. Slika 5 prikazuje vzroke za izpad informacijske podpore, kot jih je pri svoji dejavnosti ugotovilo podjetje Ontrack Data International, ki se ukvarja z restavriranjem računalniških podatkov (Toigo, 2000, str. 51). Tudi Gartner je v svoji anketi, izvedeni leta 2001 med organizacijami po vsem svetu, prišel do podobnih ugotovitev, čeprav se odstotki nekoliko razlikujejo. Slika 6 prikazuje izsledke Gartnerjeve raziskave (Wheatman, 2001).



Slika 5: Glavni vzroki izpada informacijske podpore (vir: Ontrack Data International, Inc.)



Slika 6: Glavni vzroki izpada informacijske podpore (vir: Gartner)

2.1.6 Verjetnost pojavljanja nepredvidenega dogodka

Pri vsem tem se postavlja vprašanje, kolikšen vpliv ima verjetnost pojavljanja nepredvidenega dogodka na odločitev o izbiri najučinkovitejših ukrepov za zagotavljanje poslovanja. Ker je za prikaz upravičenosti stroškov za izvajanje teh ukrepov lažje delati s številkami, obenem pa je verjetnost nepričakovanih dogodkov praktično nemogoče določiti, nekatere metodologije navajajo približne verjetnosti. Pri tem izhajajo iz zavarovalniških izračunov ali pa postavljajo

verjetnost takega dogodka na »enkrat v sto letih« ali 1/100, kar naj bi bilo nekakšno splošno povprečje (Toigo, 1996, str. 111). Škoda, ki naj bi jo taki nepredvideni dogodki povzročili, je bila potem statistično izražena v obliki produkta med verjetnostjo dogodka in velikostjo povzročene škode, pri čemer obstajajo različne variante izračunov (Toigo, 1996, str. 100, 101).

Kljub temu da je bil tak način izračunavanja preprost in je dal na videz jasno primerjavo med potencialno škodo in stroški, potrebnimi za izvedbo ukrepov za zagotavljanje poslovanja, pa so bili ti izračuni pravzaprav zelo približni. Določitev verjetnosti pojavljanja nepredvidenih dogodkov je temeljila na precej poljubnih ocenah, ki so lahko posledično vodile do zelo različnih rezultatov vrednotenja potencialne škode. Poleg tega tak način izračunavanja ne upošteva dovolj možnosti, da bi organizacija zaradi posledic predolge prekinitve poslovanja morala prenehati poslovati, kar je, kot je bilo predstavljeno v uvodu, kar precej verjetna možnost. Zato se v zadnjem času vse bolj uveljavlja prepričanje, da je razmišljanje o verjetnosti pojavljanja nepričakovanega kritičnega dogodka nesmiselno in da se je treba osredotočiti le na posledice, ki bi jih tak dogodek lahko imel na poslovanje organizacije (Toigo, 2000, str. 50, Rothstein, 2002).

2.1.7 Analiza tveganja v slovenski policiji

V slovenski policiji je bila leta 2001 izdelana analiza tveganja, katere cilj je bil zbrati podatke o ključnih poslovnih procesih, informacijski podpori teh procesov, razpoložljivosti njenega informacijskega sistema in nevarnostih, ki mu pretijo. Analiza je bila narejena z namenom ugotoviti stopnjo prilagojenosti informacijskega sistema slovenske policije zahtevam Schengenskega sporazuma, zato je bila omejena le na osrednje policijske dejavnosti z možnostjo poznejše dopolnitve z drugimi podpornimi poslovnimi procesi. V analizi je bilo zajetih devet ključnih dejavnosti in sedem aplikacij, ki te dejavnosti podpirajo.

Informacijsko telekomunikacijski sistem policije (ITSP) je zasnovan centralizirano, tako da se večina najpomembnejših aplikacij izvaja na centralnem računalniku, na katerega so po najetih vodih povezani uporabniki na posameznih policijskih postajah. Centralni računalniški sistem je lociran v Ljubljani, kjer se nahajajo tudi drugi osrednji informacijski sistemi. Policijske uprave v telekomunikacijskem pogledu delujejo kot koncentratorji povezav do policijskih postaj na svojem območju, tako da je v tem pomenu ITSP organiziran trinivojsko: osrednja lokacija – policijske uprave – policijske postaje. Na policijskih upravah in večini policijskih postaj so nameščena lokalna računalniška omrežja. Precej uporabnikov ima poleg dostopa do centralnega računalnika omogočen tudi dostop do interneta.

Evidentirane nevarnosti, ki pretijo delovanju ITSP, so bile zaradi različne metodologije za njihovo preprečevanje razdeljene v nevarnosti zunanjega in notranjega izvora. Pri evidentiranju nevarnosti je bila pozornost namenjena predvsem prvima dvema nivojema.

Zunanje nevarnosti

- požar
- potres
- večji izpad napajanja
- izpad telekomunikacijskih povezav
- računalniški vdori/virusi

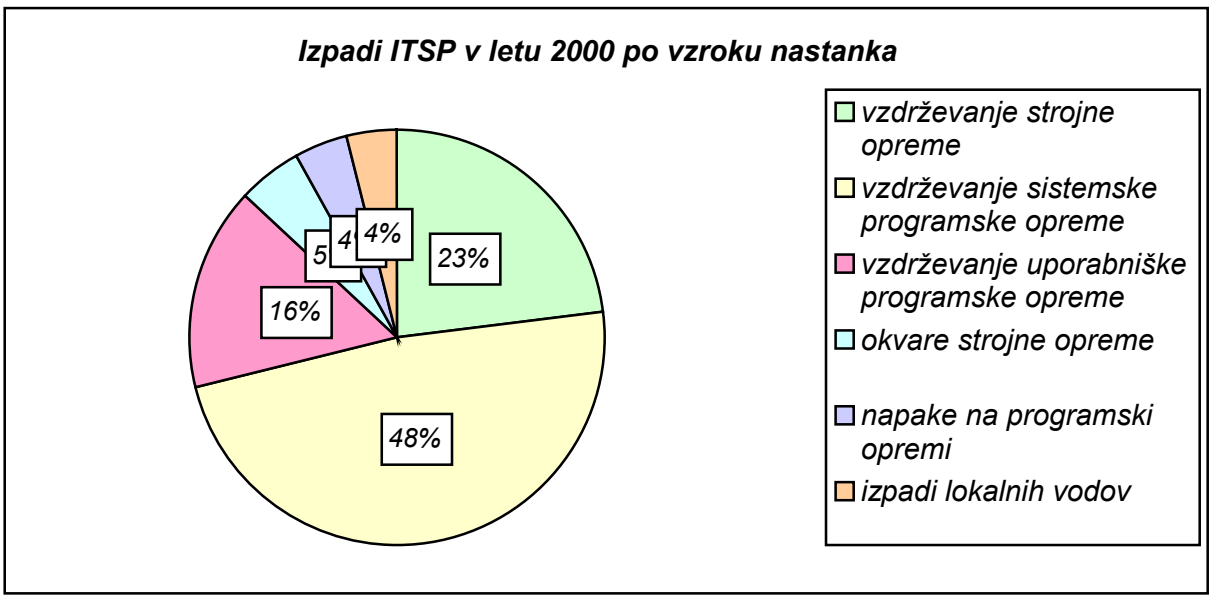
Notranje nevarnosti

- požar
- okvare strojne opreme
- poškodbe prostorov in napeljav
- nenamerne napake zaposlenih
- sabotaže

Vir: Rihar, Turk, 2001

2.1.7.1 Izpadi informacijsko telekomunikacijskega sistema policije

Narejen je bil tudi pregled izpadov informacijske podpore. Pri tem kaže upoštevati, da se izpadi na osrednji lokaciji spremljajo zelo natančno, medtem ko so trajanja izpadov na nižjih nivojih le ocenjena. Na osrednji lokaciji in najetih vodih je prišlo tudi do nekaterih okvar, ki pa jih uporabniki niso zaznali zaradi nameščenih redundantnih zmogljivosti. Na sliki 7 so prikazani izpadi ITSP leta 2000, razdeljeni glede na vzrok nastanka. Izpadi na tretjem nivoju, ki se v grafikonu odražajo predvsem v kategorijah »okvare strojne opreme« in »izpadi lokalnih vodov«, so se med različnimi policijskimi postajami zelo razlikovali, tako da so prikazani povprečni časi. Na nekaterih lokacijah je skupni delež teh dveh kategorij lahko dosegel tudi 20 odstotkov, medtem ko dela uporabnikov okvare na lokalnih vodih sploh niso prizadele. Zaradi centralizirane zasnove ITSP je večina, več kot 90 odstotkov izpadov, nastala na centralnem računalniškem sistemu.



Slika 7: Izpadi ITSP leta 2000 po vzroku nastanka (Vir: Rihar, Turk, 2001)

Iz grafikona se vidi, da je kar 87 odstotkov izpadov nastalo kot posledica vzdrževalnih posegov na strojni ali programski opremi. V vseh primerih je šlo izpade, ki so nastali kot posledica napovedanih zaustavitev zaradi širitev, rednih popravil ali zamenjave strojne opreme ter rednega vzdrževanja lastne uporabniške programske opreme. Z izjemo nekaterih lokacij, ki so jih prizadeli daljši izpadi lokalnih vodovnih povezav, so leta 2000 tudi vsi izpadi, daljši od šestih ur, nastali kot posledica vzdrževanja, nadgradnje ali zamenjave strojne opreme, bodisi na osrednji lokaciji bodisi na enem od nižjih nivojev. Ti podatki jasno kažejo, kolikšen pomen so imeli vzdrževalni posegi na splošno razpoložljivost ITSP.

2.2 Analiza vpliva na poslovanje

Zbiranju podatkov sledi analiza. Analiza mora dati odgovor na vprašanje kateri poslovni procesi so za poslovanje organizacije najbolj pomembni in bi njihova prekinitev lahko resno zmanjšala uspešnost organizacije ali celo ogrozila njen nadaljnji obstoj. Z razvrstitvijo poslovnih procesov po kritičnosti se hkrati po istem kriteriju razvrščajo tudi deli poslovnega informacijskega sistema, ki te procese podpirajo.

Na podlagi analize se za posamezne dele informacijskega sistema določita ciljna točka restavriranja podatkov (*Recovery Point Objective - RPO*) in ciljni čas vzpostavitve delovanja (*Recovery Time Objective - RTO*). Ciljni čas vzpostavitve delovanja sistema je najdaljše trajanje izpada sistema, ki ga organizacija še lahko dopusti, ne da bi resneje ogrozila svoje poslovanje. Ciljna točka restavriranja podatkov je najbolj oddaljena točka v preteklosti, do katere je še dopustno restavrirati podatke, tako da ponazarja največjo količino podatkov, ki jih organizacija še lahko izgubi brez resnejših posledic. Oba cilja pomenita temeljno merilo za izbiro vrste in obsega ukrepov, ki jih je treba uvesti za zagotavljanje delovanja poslovnega informacijskega sistema organizacije.

2.2.1 Kriteriji za razvrstitev poslovnih procesov

Kateri so tisti kriteriji, ki odločajo o pomembnosti posameznih poslovnih procesov v organizaciji? Hiles navaja naslednja splošna področja, v okviru katerih je treba vrednotiti njihov pomen, pri čemer poudarja, da so meje med temi področji dostikrat zabrisane in nejasne, in je zato jasno razvrščanje v nekaterih primerih nemogoče (Hiles, 2002):

- življenje in varnost,
- politika in marketing,
- finance,
- pogodbe in zakonodaja,
- kakovost.

Younker navaja naslednje vrste vplivov, ki jih lahko imajo različne prekinitve poslovnih procesov na organizacijo (Younker, 2002):

- ***finančni:*** neposredna izguba dohodka zaradi prekinitve,
- ***strateški:*** vpliv na pričakovane dohodke, na primer zaradi izgube intelektualne lastnine ali kupcev,
- ***zmanjšan ugled:*** izguba zaupanja kupcev in drugih strank,
- ***operativni:*** zmanjšana sposobnost sprejema naročil ali dobave proizvodov,
- ***pogodbeni, zakonodajni:*** kazni zaradi neizpolnitve pogodbenih ali zakonskih obveznosti.

Gartner je v svoji raziskavi, ki se sicer nanaša na mala in srednje velika ameriška podjetja, opredelil naslednje kategorije stroškov, ki nastanejo kot posledica zaustavitve poslovnih procesov (Scott, Browning, 2002):

- ***produktivnost:***
  - število prizadetih delavcev,
  - število ur prekinitve;
- ***dohodek:***
  - neposredna izguba,
  - izguba prihodnjega dohodka,
  - izguba investicijskih sredstev,
  - kazni zaradi neizpolnjevanja pogodbenih obveznosti;
- ***zmanjšan ugled:***
  - pri kupcih,
  - pri dobaviteljih,
  - pri poslovnih partnerjih,
  - na finančnih trgih,
  - pri bankah;
- ***finančni učinek:***
  - izguba popustov,
  - prekinitev denarnega toka,
  - višje garancije,
  - nižja cena delnic;
- ***drugi stroški:***
  - začasna delovna sila,
  - stroški nadurnega dela,
  - najem nadomestne opreme,
  - dodatni distribucijski stroški,
  - zakonske obveznosti;

2.2.2 Stroški prekinitve

Najbolj na splošno je mogoče razdeliti stroške na kratkoročne ali neposredne, ki začnejo nastajati takoj, ko se pojavi prekinitev, in dolgoročne ali posredne, ki nastanejo pozneje kot sekundarna posledica prekinitve. Neposredne stroške je navadno mogoče dokaj natančno finančno oceniti, pri čemer pa je treba paziti, da zaradi nejasnih meja potencialnih posledic ne upoštevamo večkrat. Neposredni stroški lahko naraščajo sorazmerno s trajanjem prekinitve, pogosto pa se povečujejo tudi nesorazmerno ali skokovito. Prav zato je zelo koristno te stroške oceniti v časovni odvisnosti.

Precej težje pa je oceniti posredne oziroma dolgoročne stroške, kot so na primer stroški povrnitve ugleda pri kupcih in poslovnih partnerjih, stroški povrnitve tržnega deleža, stroški izgube vrednosti blagovne znamke ipd.. Ti stroški se začnejo pojavljati šele ob daljši prekinitvi poslovnega procesa, pri čemer pa je kritično trajanje prekinitve zelo težko oceniti, saj se tako kritični čas prekinitve kot potencialni obseg posrednih stroškov med različnimi deli poslovnega procesa in v različnih panogah lahko močno razlikujejo. Kritični čas prekinitve je navadno najkrajši pri poslovnih procesih, ki služijo za komuniciranje s kupci, posredni stroški v takih primerih pa so na splošno višji v panogah z večjo elastičnostjo povpraševanja. Pomemben element pri razvrščanju poslovnih procesov po kritičnosti so tudi zakonske in pogodbene obveznosti, ki jih je treba spoštovati in ki v nekaterih primerih zelo natančno določajo najdaljši še dovoljeni čas prekinitve delovanja katerega od poslovnih procesov.

V nekaterih organizacijah, na primer v javnih institucijah, so stroški prekinitve večinoma zelo težko merljivi in niti niso tako pomembni, zato pa so precej bolj pomembne druge, predvsem posredne posledice prekinitve delovanja. Pri državnih institucijah na primer povzroči prekinitev katerega od ključnih poslovnih procesov padec ravni podpore občanom in s tem padec njihove pravne in siceršnje varnosti, kar je na splošno zelo težko merljiva kategorija. Pri nekaterih državnih institucijah, kot sta na primer vojska ali policija, lahko prekinitev delovanja v nekaterih bolj izpostavljenih primerih pomeni celo grožnjo za delovanje in obstoj države.

2.2.3 Razvrstitev poslovnih procesov

Po končani analizi vpliva na poslovanje je posamezne poslovne procese zaradi lažje analize smotrno razvrstiti po stopnji njihove kritičnosti na več skupin. Tako se razdelijo tudi njihove podporne aplikacije, s tem pa tudi poslovni informacijski sistem na več delov, ki zahtevajo različno obravnavo glede na zahtevano stopnjo zagotavljanja delovanja. Razvrstitev je uporabna tudi za določanje potrebnega dogovora o ravni storitev (*Service Level Agreement – SLA*) v primeru, da je poslovni proces deloma ali v celoti prepuščen zunanjemu izvajalcu.

Gartner priporoča razdelitev poslovnih procesov v štiri kategorije glede na stopnjo njihove kritičnosti za poslovanje organizacije. V tabeli 1 so prikazane štiri kategorije, kot jih je opredelil Gartner, z zelo natančno določenimi pripadajočimi potrebnimi ravnmi storitev in primeri poslovnih procesov, ki sodijo v posamezno kategorijo (Scott, Krischer, 2002).

Kategorija	***Primeri poslovnih procesov***	***Potrebne ravni storitev***
1.	• *odnosi s strankami/partnerji* • *procesi, kritični za pridobivanje dohodka*	• *24x7 delovanje* • *99,9 % razpoložljivost (< 45 min/mes.)* • *RTO < 2 uri; RPO = 0*
2.	• *manj kritični procesi za pridobivanje dohodka* • *preskrbovalna veriga*	• *24x7 delovanje* • *99,5 % razpoložljivost (< 3,5 ure/mes.)* • *RTO 8-12 ur; RPO 4 ure*
3.	• *organizacijsko pisarniško poslovanje*	• *18x7 delovanje* • *99 % razpoložljivost (< 5,5 ure/mes.)* • *RTO 3 dni; RPO 1 dan*
4.	• *oddelčni procesi*	• *24x6 delovanje* • *98 % razpoložljivost (< 13,5 ure/mes.)* • *RTO 5 dni; RPO 1 dan*

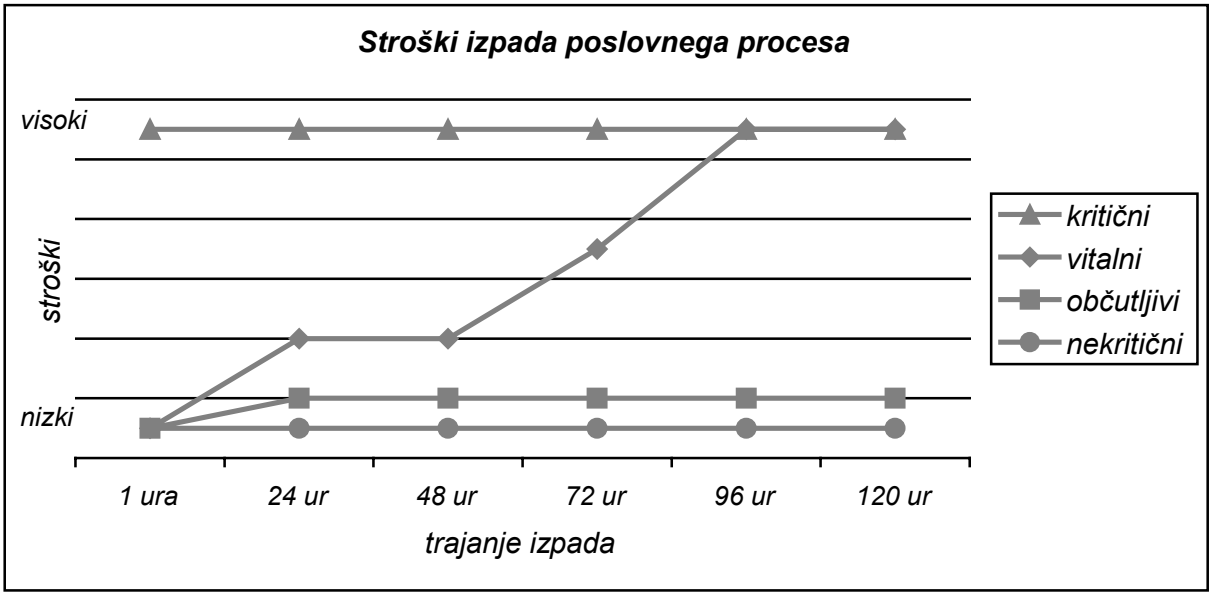
Tabela 1: Razvrstitev poslovnih procesov po kritičnosti (Vir: Gartner)

Toigo podobno razvršča poslovne procese po kritičnosti v štiri različne skupine, ki jih opredeli opisno. Tudi to razdelitev je mogoče uporabiti za razvrščanje elementov poslovnega informacijskega sistema, ki podpirajo navedene poslovne procese (Toigo, 2000, str. 46-48).

- ***Kritični***. To so procesi, katerih prekinitev lahko organizaciji povzroči nepopravljive posledice že v zelo kratkem času. Takih procesov organizacija ne more izvajati, če nima na razpolago popolnih nadomestnih zmogljivosti.
- ***Vitalni.*** To so procesi, katerih prekinitev lahko organizacija za krajši čas, na primer 48 ur, dopusti pod pogojem, da se potem v popolnosti obnovijo. Takih procesov ni mogoče izvajati na alternativen način ali pa je to mogoče le zelo kratek čas in z velikimi stroški. Če v dveh do petih dneh podpora teh procesov ni v celoti vzpostavljena, ima njihova prekinitev za organizacijo podobne posledice, kakršne veljajo za kritične procese.

- ***Občutljivi***. To so procesi, ki jih je mogoče dlje časa ob sprejemljivih stroških izvajati tudi na alternativen način, vendar pa je treba po prehodu na normalno poslovanje podatke in postopke v celoti restavrirati.
- ***Nekritični***. So procesi, ki jih lahko organizacija brez posebne škode pogreši tudi dlje časa in ne zahtevajo restavriranja ali pa je to relativno poceni.

Značilna časovna razporeditev stroškov, ki nastanejo pri različnih kategorijah poslovnih procesov, je prikazana na sliki 8.



Slika 8: Stroški izpada poslovnega procesa (Vir: Toigo, 2000, str. 48)

2.2.4 Ugotovitve analize vpliva na poslovanje

Smisel analize vpliva na poslovanje je predvsem v tem, da se evidentirajo in ocenijo vse ali vsaj večina posledic izpada posameznega poslovnega procesa. Ker gre za oceno, pri analizi nima smisla pretiravati z natančnostjo merjenja stroškov, saj bi bilo to predrago in bi trajalo predlogo časa, poleg tega pa vseh posledic niti ni mogoče natančno cenovno ovrednotiti, in je zato marsikdaj treba upoštevati tudi vrednostne ocene. Analiza mora biti dovolj pregledna, preprosta in razumljiva, da jo je mogoče pozneje brez težav dopolnjevati s poslovnimi, organizacijskimi ali tehničnimi spremembami, ki nastanejo v organizaciji.

V nekaterih primerih je dobro pripraviti tudi preprost pregled izsledkov analize vpliva na poslovanje, kar je mogoče izvesti na več načinov, pri čemer je pomembno predvsem to, da je pregled preprost, a dovolj popoln, da daje višjemu menedžmentu podlago za sprejemanje

odločitev o uvajanju pogojev za zagotavljanje delovanja poslovnega informacijskega sistema. Primer preproste predstavitve v tabelarični obliki, pri kateri so za izhodišče izbrani organizacijski poslovni procesi, je prikazan v tabeli 2.

Poslovni proces	***Elementi informacijske podpore***	***Tveganje***	***Verjetnost****	***Vpliv na poslovanje****	***Dejavnik tveganja***
1.Prodaja po internetu	***1. strežnik***	*okvara*	*2*	*7*	*14*
		požar	*1*	*4*	*4*
		potres	*1*	*3*	*3*
		vdor	*3*	*5*	*15*
		vzdrževanje	*2*	*6*	*12*
		…			
	2. diski	*okvara kontr.*	*1*	*6*	*6*
		okvara diska	*3*	*2*	*6*
		požar	*1*	*3*	*3*
		vzdrževanje	*2*	*4*	*8*
		…			
	3. aplikacija	*okvara*	*1*	*3*	*3*
		vzdrževanje	*2*	*1*	*2*
		…			
	4. ...				
2….					

** Vrednosti med 1 (zalo majhna) in 10 (zelo velika)*

Tabela 2: Primer tabele analize vpliva na poslovanje

Tabelo je v opznejši fazi oblikovanja okrevalne strategije mogoče dopolniti tudi s predlaganimi protiukrepi ter novimi vrednostmi potencialnega vpliva na poslovanje in dejavnika tveganja, kot je prikazano v tabeli 3.

Elementi informacijske podpore	***Tveganje***	***Protiukrep***	***Novi vpliv na poslovanje****	***Novi dejavnik tveganja***
1. strežnik	*okvara*	*redundantni strežnik*	*1*	*2*
	požar	*protipožarna zaščita*	*2*	*2*
	potres	*-*	*3*	*3*
	vdor	*požarni zid*	*2*	*6*
	vzdrževanje	*redundantni strežnik*	*0*	*0*
2. ...				

** Vrednosti med 1 (zalo majhna) in 10 (zelo velika)*

Tabela 3: Dodatek k tabeli analize vpliva na poslovanje

2.2.5 Analiza vpliva na poslovanje v slovenski policiji

V slovenski policiji je bila narejena analiza poslovanja za osrednje dejavnosti, ki so bile zajete v analizi tveganja. Zaradi narave dela pri tem ni bila narejena stroškovna ocena, pač pa se je pri analizi izhajalo le iz zahtev, ki so jih dolžne spoštovati podpisnice Schengenskega sporazuma. Od devetih analiziranih dejavnosti so bile tri opredeljene kot kritične z RTO krajšim od 6 ur in z RPO pod 15 minutami, tri dejavnosti kot občutljive z RTO pod 24 urami in RPO pod 12 urami in tri kot vitalne z RTO do 5 dni in RPO pod 48 urami. Skladno s to razdelitvijo so bile razdeljene tudi pripadajoče aplikacije tako, da so bile tri opredeljene kot kritične, ena kot občutljiva in tri kot vitalne. Ker je ITSP zasnovan skoraj povsem centralizirano, se skoraj vse aplikacije, ki podpirajo osrednje dejavnosti, med njimi tudi vse kritične, izvajajo na centralnem računalniku in so podprte z osrednjo telekomunikacijsko infrastrukturo.

Relativno visoko kritičnost evidentiranih poslovnih procesov in povezanih aplikacij gre pripisati dejstvu, da so bile v analizo zajete le osrednje policijske dejavnosti, ki se tako ali drugače navezujejo na problematiko približevanja Evropski zvezi. Drugi, pretežno podporni poslovni procesi, ki bodo v analizo zajeti pozneje, bodo v povprečju nedvomno dosegali nižje stopnje kritičnosti.

3 Preventivna dejavnost

Preventivno delovanje zajema zelo širok spekter dejavnosti, ki jih v večjem ali manjšem obsegu za zaščito svojih informacijskih sistemov izvajajo vse organizacije. Preventivna dejavnost je pomembna predvsem zato, ker je preprečevanje izrednih dogodkov na splošno cenejše, kakor odpravljanje njihovih posledic, poleg tega pa tudi zato, ker nobena, še tako popolna pomožna rešitev, ne more v celoti nadomestiti funkcionalnosti prvotnega informacijskega sistema. Prav zato je treba v postopku uvajanja pogojev za zagotavljanje delovanja informacijskega sistema evidentirati vse preventivne dejavnosti, ki jih organizacija že izvaja, ovrednotiti njihov učinek in v skladu z ugotovitvami analize tveganja po potrebi predlagati njihovo spremembo ali dopolnitev.

V okvir preventivne dejavnosti organizacije v širšem pomenu seveda sodijo prav vse dejavnosti, ki so namenjene uvajanju pogojev za zagotavljanje delovanja informacijskega sistema. Vendar se bo v okviru tega dela pojem preventivnega delovanja nanašal le na tisti del

preventivnih dejavnosti, ki so namenjene preprečevanju izrednih dogodkov, oziroma, pogosteje, zmanjšanju verjetnosti njihovega pojavljanja ter omilitvi njihovega obsega in ostrine. S stališča zaščite informacijskega sistema organizacije pa lahko tako opredeljene preventivne dejavnosti razdelimo v dva sklopa.

V prvi sklop sodijo preventivne dejavnosti, ki so namenjene fizični zaščiti kritičnih infrastruktur, kot so objekti, prostori, napeljave ali naprave. Obseg in vrsto teh preventivnih dejavnosti v organizaciji največkrat določajo zakonske obveznosti ali splošna varnostna politika organizacije, odvisne pa so tudi od okoliščin, v katerih organizacija deluje. Tovrstne dejavnosti bolj ali manj izvajajo vse organizacije, zaradi njihove narave in visokih stroškov njihovega izvajanja pa se med uvajanjem pogojev za zagotavljanje delovanja informacijskega sistema navadno lahko le evidentirajo ter se upošteva njihov vpliv na zmanjšanje tveganja.

Drugi sklop preventivnih dejavnosti je vezan neposredno na informacijski sistem organizacije in ga tvorijo postopki, ki so namenjeni njegovi logični zaščiti pred vdori. Ta del preventivnih dejavnosti je odvisen predvsem od varnostne politike in kulture organizacije in postaja z vedno tesnejšim informacijskim povezovanjem organizacij z okolico vse pomembnejši. Organizacije največkrat ščitijo dostop do svojih informacijskih sistemov predvsem zaradi bojazni pred nepooblaščeno uporabo občutljivih podatkov, manj pa zaradi preprečevanja vdorov, ki ogrožajo samo delovanje sistema. Uvajanje dejavnosti, namenjenih logični zaščiti sistema, ni drago, zaradi hitrih tehnoloških sprememb pa zahteva visoko raven strokovnega znanja in neprestano prilagajanje na nove nevarnosti.

Pomembna prvina preventivnega delovanja je tudi skrb za delavce, ki so tako ali drugače povezani z delovanjem informacijskega sistema, kamor sodijo izobraževanje, varnostno osveščanje in nadzor zaposlenih. Izobraževanje zaposlenih je zelo pomembno zaradi hitrih tehnoloških sprememb na informacijskem in telekomunikacijskem področju, in to tudi tedaj, ko je oskrbovanje informacijskega sistema prepuščeno zunanji organizaciji. Varnostno osveščanje in nadzor pa pripomoreta k spoštovanju in ustreznem uresničevanju sprejetih varnostnih standardov v organizaciji. Pogosto se namreč dogaja, da je razkorak med sprejeto in dejansko uresničevano varnostno politiko dokaj velik.

Področje načrtovanja in uresničevanja preventivnih dejavnosti je izjemno široko in bi njegova podrobnejša obravnava daleč presegla okvir tega dela. Uresničevanje preventivnih dejavnosti je v večjih organizacijah odvisno od organizacijske varnostne politike, ki sledi tudi drugim varnostnim ciljem in je navadno ni mogoče bistveno spreminjati. Pomembno je tudi spoznanje, da ukrepi za preprečevanje nevarnosti slednjih ne morejo povsem odpraviti, pač pa lahko le zmanjšajo verjetnost njihovega pojavljanja oziroma, kar je morda še pomembneje, zmanjšajo obseg najverjetneje nastale škode. V nadaljevanju bodo navedene nekatere glavne značilnosti področja preventivnih dejavnosti, na katera je treba usmeriti pozornost pri analizi tveganja.

3.1 Fizična zaščita

Fizična zaščita je pomemben varnostni preventivni element za zagotavljanje delovanja informacijskega sistema in jo je v tem pomenu treba upoštevati pri izdelavi analize tveganja. V organizacijah so za tovrstne dejavnosti odgovorne posebne varnostne službe, bodisi notranje bodisi zunanje, ki lahko dajejo ustrezne informacije o njihovem obsegu in kakovosti. V to skupino preventivnih dejavnosti sodijo ustrezni ukrepi za zaščito kritičnih infrastruktur, kot so na primer:

- sistemi za detekcijo dima v prostorih z informacijsko opremo,
- sistemi za gašenje požarov in protipožarna zaščita,
- sistemi za zagotavljanje neprekinjenega napajanja,
- fizična zaščita dostopa do prostorov z informacijsko opremo,
- sistemi za detekcijo izliva vode,
- zaprti sistemi za zaščito informacijske opreme znotraj prostorov,
- ukrepi za zmanjšanje nevarnosti požara ter onesnaženja z drugimi onesnaževalci idr.

V širšem opmenu sodijo v to skupino preventivnih dejavnosti že izbira lokacije za postavitev računalniškega centra in konstrukcijske značilnosti objekta, v katerem se center nahaja, če je mogoče na te lastnosti kakor koli vplivati. Navadno so te lastnosti na primarni lokaciji bolj ali manj nespremenljive, zato pa je mogoče nanje vplivati pri izbiri morebitne nadomestne lokacije.

3.1.1 Protipožarni sistemi

Sistemi za gašenje požarov s halonom, ki so bili včasih precej pogosti, se zaradi nevarnosti, ki jih prinašajo, danes redkeje uporabljajo. Zamenjujejo se z drugimi sistemi, ki uporabljajo manj nevarne kemikalije (Toigo, 2000, str. 75). Pogosto se uporabljajo tudi dimni detektorji, ki lahko v kombinaciji s stalnim človeškim nadzorom (operaterji v sistemskem prostoru) zagotavljajo podobno stopnjo zaščite. Dodatno protipožarno zaščito pomenijo tudi konstrukcijske karakteristike prostorov z informacijskimi napravami, ognjevarne predelne stene, protipožarna vrata ipd. K protipožarni varnosti precej prispevata tudi praksa in spoštovanje protipožarnih predpisov s strani zaposlenih v organizaciji.

Protipožarni sistemi so dokaj učinkoviti pri požarih, ki nastanejo znotraj informacijskih centrov, medtem ko so pri požarih, ki nastanejo zunaj njih, manj učinkoviti, saj ne morejo preprečiti poškodovanja opreme zaradi vročine, dima in strupenih plinov. Zato se v zadnjem času vse pogosteje uporabljajo zaprti sistemi (»prostori znotraj prostorov«), posebne nepredušno zaprte kletke, v katerih je nameščena informacijska oprema. Te kletke imajo

lastno protipožarno zaščito in učinkovito varujejo naprave tudi pred vročino in nevarnimi plini iz okolice.

Z učinkovito protipožarno zaščito in dimnimi detektorji je mogoče zmanjšati verjetnost nastanka požara v informacijskem prostoru in njegov obseg, vendar pa je treba upoštevati, da še tako učinkovita protipožarna zaščita ne more povsem izključiti možnosti požara. Zato je treba pri analizi tveganja računati z možnimi posledicami požara ne glede na obstoj in kakovost protipožarne zaščite. Seveda pa je treba pri tem upoštevati verjetni obseg in posledice požara, ki so glede na stopnjo protipožarne zaščite v organizaciji lahko zelo različni.

3.1.2 Sistemi za zagotavljanje neprekinjenega napajanja

Zelo pomemben element preventivne zaščite informacijskih sistemov so tudi sistemi za zagotavljanje neprekinjenega napajanja (*Uninterruptible Power Supply – UPS*). Večina informacijske strojne opreme, še posebno procesne enote in diskovni sistemi, so zelo občutljivi na nenaden izpad električne energije, zato verjetno ni organizacije, ki ne bi uporabljala katere od naprav za neprekinjeno napajanje.

Vsi današnji sistemi za neprekinjeno napajanje slonijo na uporabi akumulatorjev, ki lahko ob izpadu električne energije iz omrežja omogočajo ustrezno napajanje strojne opreme. Na splošno obstajata dve vrsti sistemov za neprekinjeno napajanje – tako imenovani »*stand-by*« sistemi, pri katerih se pomožno napajanje vključi le ob izpadu napajanja iz omrežja, in tako imenovani »*on-line*« sistemi, preko katerih je strojna oprema stalno (posredno) priključena na omrežje. Slednji, ki imajo pred prvimi to prednost, da obenem služijo tudi kot stabilizatorji omrežne napetosti, se uporabljajo večinoma za večje sistema.

Namen naprav za neprekinjeno napajanje je predvsem v tem, da omogočajo premostitve za kratkotrajne izpade v javnem energetskem omrežju in da ob dolgotrajnejšem izpadu energije iz omrežja zagotovijo informacijski strojni opremi dovolj časa, da se pravilno zaustavi. Če želi organizacija premostiti tudi dolgotrajne izpade energetskega omrežja, mora zagotoviti napajanje svoje informacijske strojne opreme z uporabo agregata. V takem primeru se lahko možnost zaustavitve informacijskega sistema zaradi izpada napajanja oceni za zelo majhno in je pravzaprav enaka možnosti, da se pokvari sam sistem neprekinjenega napajanja.

3.1.3 Fizično varovanje prostorov

Večina organizacij ima prostore s kritično strojno opremo fizično zaščitene pred vstopom nepooblaščenih oseb predvsem zaradi zaščite podatkov, pa tudi zaradi varnosti delovanja informacijskega sistema. Tistim organizacijam, ki svojih zbirkah vodijo osebne ali zaupne podatke, pa predpisuje način varovanja takih podatkov in opreme, kjer se podatki nahajajo,

zakonodaja, ki ureja ravnanje s tovrstnimi podatki. Dodatno varovanje dostopa do kritične strojne opreme zagotavlja tudi stalna navzočnost operaterjev v tistih računalniških centrih, kjer je to potrebno.

3.2 Logična zaščita

Logično zaščito sestavljajo vse dejavnosti, ki so namenjene zaščiti informacijskega in telekomunikacijskega sistema organizacije pred nepooblaščenimi dostopi in računalniškimi vdori. V zadnjih letih, ko so poslovni informacijski sistemi čedalje tesneje povezani z okoljem, postaja problem varnosti čedalje bolj pereč. Seznam možnih nevarnosti in groženj, predvsem z interneta, se neprestano spreminja in podaljšuje. Različne organizacije, kot sta na primer Computer Science and Telecommunication Board ali SANS Institute, neprestano spremljajo dogajanje na svetovnem spletu in o ugotovitvah poročajo na svojih spletnih straneh.

Za zaščito informacijskega sistema pred nepooblaščenimi dostopi sta pomembna predvsem dva varnostna elementa: nadzor vstopa v sistem in varovanje komunikacijskih poti, po katerih potujejo podatki. Za varovanje podatkov pred nepooblaščenim vpogledom sta enako pomembna oba navedena elementa, medtem ko je za zagotavljanje delovanja sistema bolj pomemben prvi.

3.2.1 Nadzor vstopa v informacijski sistem

V časih, ko so bili informacijski sistemi centralizirani, so bile možnosti za nepooblaščeni vstop v tak sistem zelo majhne, saj so bile komunikacije organizirane strogo hierarhično in centralno nadzirane. Vdori v take sisteme so bili zaradi zaprte komunikacijske arhitekture praktično nemogoči, tudi virusov za ta okolja ni bilo. Vse to velja za informacijske sisteme organizirane okrog centralnih računalnikov še danes, vendar le, če ti sistemi niso neposredno povezani z okoljem.

Pozneje, ko so se v sisteme začeli vključevati mrežni strežniki in osebni računalniki kot delovne postaje, so se možnosti vstopa močno povečale, hkrati pa se je povečala tudi ranljivost sistemov zaradi pojavljanja računalniških virusov. Virusi so prihajali v sistem večidel z uporabo disket, s katerimi so zaposleni prenašali podatke, znotraj sistema pa lahko tudi po elektronski pošti. Tako širjenje virusov je bilo mogoče preprečiti bodisi s preprečevanjem vsesplošnega prenašanja podatkov po disketah bodisi z uporabo protivirusnih programov, še najpogosteje pa s kombinacijo obojega. Računalniške povezave med organizacijami so bile redke in so bile konfigurirane za računalniško izmenjavo podatkov z zaprtimi protokoli z zelo omejenim dosegom, zato so bili vdori v sistem po teh povezavah praktično nemogoči.

Z razmahom interneta in vse tesnejšimi povezavami med organizacijami ter med organizacijami in strankami sta nastali dve novi nevarnosti. Prvič se je zaradi povezave informacijskih sistemov na internet in zaradi splošne uporabe internetne elektronske pošte izjemno povečala možnost širjenja virusov in drugih oblik škodljive programske kode. Druga nevarnost, ki se je pojavila zaradi uporabe splošnega komunikacijskega protokola TCP/IP in njegovih slabosti, pa je možnost vdora v informacijski sistem oziroma možnost vplivanja na njegovo delovanje od zunaj.

Obramba proti virusom, ki prihajajo s spleta, je težka zaradi neprestanega pojavljanja novih virusov in zaradi njihovega zelo hitrega širjenja. Proti virusom se je mogoče braniti z uporabo požarnih zidov, s katerimi je mogoče preprečiti vstop programske kode v informacijski sistem, z obvezno uporabo protivirusnih programov v sistemu ali s kombinacijo obeh metod. Zelo koristna za varnost informacijskega sistema organizacije je tudi delitev sistema na dva dela, od katerih je eden lahko v stiku z okoljem, drugi pa ne. Med obema deloma sistema se postavi zelo strog protokol izmenjave podatkov, ki je navadno organiziran tako, da notranji, varni del sistema nadzira pretok podatkov v obe smeri.

Podobno kot obramba pred virusi je organizirana tudi obramba pred vdori. Najpomembnejši element te obrambe so požarni zidovi, ki nadzirajo dostop iz okolice in filtrirajo promet v informacijski sistem organizacije. Za zaščito pred vdori mora biti kakovost požarnih zidov bistveno večja, kot je to potrebno pri obrambi pred virusi, zato se v ta namen navadno uporablja namenska strojna oprema, ki je dražja, a učinkovitejša od programskih požarnih zidov. Poleg tega se pogosto uporabljajo tudi posebni programi, ki neprestano pregledujejo promet skozi informacijski sistem in opozarjajo na poskuse vdorov. Dodatno zaščito pred vdori omogoča, podobno kot pri obrambi pred virusi, tudi delitev informacijskega sistema na »varni« ali zaprti del in »nevarni« ali odprti del.

Obramba informacijskega sistema pred virusi in vdori je tehnološko izjemno zahtevno delo, ki zahteva neprestano preverjanje in izboljševanje obstoječih obrambnih mehanizmov. Prav zato morajo imeti organizacije, ki želijo resno poskrbeti za varnost svojega informacijskega sistema, oblikovane posebne službe, katerih naloga je nenehno posodabljati obrambne sisteme in jih prilagajati na nove nevarnosti iz kibernetskega okolja. Taka služba je oblikovana tudi v slovenski policiji.

Učinkoviti obrambni mehanizmi lahko sicer bistveno zmanjšajo verjetnost vdora in obseg možne škode, vendar pa je mogoče trditi, da noben informacijski sistem ni povsem varen pred vdori, ne glede na uporabljeno tehniko zaščite. Zato je treba možnost delnega ali popolnega izpada delovanja informacijskega sistema zaradi tovrstnih razlogov pri analizi tveganja vsekakor upoštevati, ne glede na uporabo preventivnih zaščitnih in kontrolnih mehanizmov.

4 Izdelava okrevalnega načrta

Okrevalni načrt je osrednji operativni dokument, v katerem so zaobseženi cilji, ki jih želi organizacija doseči z uvajanjem pogojev za zagotavljanje delovanja svojega informacijskega sistema, ter postopki, ki jih mora izvesti za dosego teh ciljev. Načrt izhaja iz izsledkov analiz tveganja in vpliva na poslovanje, obstoječih preventivnih dejavnosti ter že uveljavljenih postopkov za zagotavljanje delovanja in odraža stopnjo pripravljenosti organizacije za reševanje te problematike.

Metodologija izdelave, obseg in natančnost načrta se od primera do primera lahko zelo razlikujejo. Največkrat dajo organizacije izdelati načrt zunanjim strokovnjakom ali strokovnim službam, ki so posebej usposobljene za izdelavo tovrstnih načrtov. Vse večje računalniške družbe, kot sta na primer IBM ali Hewlett-Packard, imajo v ta namen oblikovane posebej usposobljene skupine, poleg tega pa obstaja tudi vrsta manjših, specializiranih podjetij in certificiranih svetovalcev. Zunanji strokovnjaki izdelajo okrevalni načrt in potrebne analize hitro in kakovostno, problem tovrstne rešitve pa je predvsem v nevarnosti, da se načrt zaradi pomanjkljivega znanja znotraj organizacije pozneje ne dopolnjuje več, in zato postane sčasoma neuporaben, ali pa je treba tudi za vzdrževanje načrta iskati zunanjo pomoč.

Zato se nekatere organizacije raje odločijo za izdelavo okrevalnega načrta z lastnimi varnostnimi in tehničnimi strokovnjaki. Tako že med izdelovanjem načrta pridobivajo potrebno znanje, ki ga lahko s pridom izkoristijo tudi pozneje pri vzdrževanju in prilagajanju načrta novim zahtevam in tehnološkim spremembam. To je ob nižji ceni izdelave tudi glavna prednost tovrstnega načina, poleg tega se načrti, ki so jih izdelali domači strokovnjaki, navadno bolj natančno prilegajo zahtevam organizacije.

Problem pri takem načinu je predvsem zelo verjetno pomanjkanje znanja in izkušenj pri domačih strokovnjakih ter iz tega izvirajoča možnost, da se v načrtu pojavijo napake ali pomanjkljivosti. Pri razvoju okrevalnega načrta znotraj organizaceije se pogosto dogaja, da tako oblikovani načrti nastajajo sproti, hkrati z uvajanjem ukrepov za zagotavljanje delovanja in ne vnaprej, kot je to značilno za načrte, ki jih prispevajo zunanji strokovnjaki. Pri izdelavi načrta si je mogoče pomagati z dokumentarnimi postopki in navodili, ki so na voljo skupaj z literaturo, ki se ukvarja s to problematiko (Fulmer, 2000, Toigo, 1995) ali s programsko opremo, s katero si je mogoče pomagati pri izvedbi posameznih faz izdelave načrta (Noakes-Fry, Diamond, 2002).

V slovenski policiji sta bili pretehtani obe možnosti izdelave okrevalnega načrta. Zaradi specifičnosti okoliščin, v katerih deluje slovenska policija, in s tem povezano potrebo po popolnem obvladovanju problematike z lastnimi ljudmi je prevladala odločitev, da se kljub pomanjkljivim izkušnjam okrevalni načrt izdela z uporabo lastnega znanja. Trenutno je izdelan le njegov grobi obris, v okviru katerega bodo izvedeni nekateri ukrepi za zagotovitev

delovanja informacijskega sistema, ki jih je zaradi časovne stiske treba vpeljati pred njegovo dokončno izdelavo, celotni načrt pa bo izdelan pozneje.

4.1 Vsebina okrevalnega načrta

O tem, kaj naj bi obsegal okrevalni načrt, se mnenja različnih avtorjev med sabo precej razlikujejo. Fulmer na primer navaja naslednjo, zelo natančno listo poglavij, ki bi se morala nahajati v načrtu (Fulmer, 2000, str. 97):

- namen načrta,
- pregled načrta (cilji, okvir, predpostavke),
- distribucijska lista,
- vzdrževanje načrta,
- način testiranja načrta,
- postopki evakuacije,
- lista obveščanja o izrednih dogodkih,
- akcijski načrt,
- spisek okrevalnih ekip (teamov),
- podpora zunanjih izvajalcev,
- podatki o procesorjih na oddaljeni (sekundarni) lokaciji,
- podatki o diskovnih zmogljivostih na oddaljeni lokaciji,
- podatki o programski opremi,
- podatki o drugi opremi,
- podatki o telekomunikacijskih povezavah,
- podatki o dokumentaciji in priročnikih,
- telefonske številke,
- klicna lista zaposlenih in nadomestnih delavcev.

Toigo poudarja, da je načrt sicer pomemben, da pa se ni treba preveč posvečati le papirni dokumentaciji, pač pa bolj uveljavljanju in osvajanju postopkov ter predvsem pripravi zaposlenih na izredne situacije (Toigo, 2000, str. 290). Okrevalni načrt naj bi tako obsegal projekte za izvedbo bistvenih postopkov kriznega menedžmenta za primer obvladovanja izredne situacije.

- ***Projekt evakuacije***

    - ***Odziv na izredno situacijo.*** Postopki odzivanja na izredne dogodke, kot so na primer postopki aktiviranja protipožarne zaščite, evakuacijski postopki ipd.

- ***Obveščanje.*** Postopki obveščanja menedžmenta in vzpostavitve kriznega obveščevalnega centra.
- ***Razglasitev izrednega dogodka.*** Postopki in navodila za oceno nastale situacije in morebitne škode ter odločitev o razglasitvi stopnje izrednega dogodka in začetku izvajanja okrevalnega načrta.

- ***Projekt vzpostavitve poslovanja***

  - ***Restavriranje sistemov.*** Postopki za ponovno vzpostavitev kritičnih aplikacij v predvidenem časovnem okviru in v skladu z načrtovano okrevalno strategijo.
  - ***Restavriranje omrežja.*** Postopki za ponovno vzpostavitev nadomestnega telekomunikacijskega omrežja v predvidenem časovnem okviru in v skladu z načrtovano okrevalno strategijo.
  - ***Restavriranje uporabniških funkcij.***
  - ***Reševanje premoženja.*** Postopki za reševanje poškodovanega premoženja, zavarovalniški postopki in ocenitev možnosti za ponovno uporabo poškodovanih objektov in naprav.

- ***Projekt vzpostavitve normalnega stanja***

  - ***Vzpostavitev normalnega stanja.*** Postopki za vračanje z nadomestnih zmogljivosti bodisi nazaj v prvotno (staro) stanje bodisi na novo stalno lokacijo.

Gartner pojmuje okrevalni načrt še precej širše in izhaja iz ugotovitve, da je prav krizni menedžment najpomembnejši v trenutku, ko se pojavi nepričakovan dogodek, ki lahko prepreči ustaljeni način poslovanja. Ustrezni način vodenja v kriznih trenutkih je tisti, ki lahko zagotovi, da bodo zaposleni, stranke, partnerji, investitorji in splošna javnost ohranili zaupanje v delovanje in nadaljnji obstoj prizadete organizacije. Načrt, ki je oblikovan po principih kriznega menedžmenta in pokriva vse štiri kritične komponente, ki jih ponazarja tabela 4, s tem dejansko iz okrevalnega načrta preraste v načrt zagotavljanja poslovanja (Younker, 2001).

	Okrevanje po nesreči (Disaster recovery)	***Okrevanje poslovanja (Business recovery)***	***Nadaljevanje poslovanja (Business Resumption)***	***Obvladovanje tveganja Contingency Planning)***
Cilj	*Kritične aplikacije*	*Kritični poslovni procesi*	*Poslovno okolje*	*Zunanji dogodek*
Problem	*Izpad lokacije ali komponente*	*Izpad lokacije*	*Izpad aplikacije*	*Zunanji dogodek, ki vpliva na poslovanje*
Izdelek	*Načrt okrevanja po nesreči*	*Načrt okrevanja poslovanja*	*Načrt alternativnih načinov poslovanja*	*Analiza možnega tveganja za poslovanje*
Primer dogodka	*Požar v računalniškem centru; okvara pomembnega strežnika*	*Izpad napajanja za celotno lokacijo*	*Izpad aplikacije letalskih rezervacij*	*Izpad pomembne dobave zaradi težav dobavitelja*
Primer možne rešitve	*Redundantna strojna oprema*	*Oddaljeni računalniški center*	*Ročno procesiranje*	*Zaloga kritičnih surovin; nadomestni dobavitelj*

Tabela 4: Komponente načrta zagotavljanja poslovanja (Vir: Gartner, 2001)

4.2 Ključni dejavniki uspešnosti

Ne glede na obliko in obseg okrevalnega načrta ter načrtovanih okrevalnih postopkov pa je zanimivo, da se njihova učinkovitost v različnih organizacijah lahko zelo razlikuje. Gartner je na podlagi proučevanja različnih primerov okrevanja po nepričakovanih uničujočih dogodkih v poslovnem svetu poskušal dognati, kateri so tisti ključni dejavniki, ki lahko zagotovijo uspeh ali povzročijo neuspeh okrevalnih načrtov. Nekateri najbolj pomembni kritični faktorji uspešnosti okrevalnih postopkov v organizaciji, do katerih je v svoji raziskavi prišel Gartner, so navedeni v nadaljevanju (Neil, 2001).

- ***Odnos višjega menedžmenta***. Zavezanost višjega menedžmenta do problematike in njegova pripravljenost za vsestransko podporo izvajanja potrebnih okrevalnih ukrepov je izjemno pomembna. Pomanjkanje interesa navadno privede do odtegovanja sredstev in ljudi s področja, kar privede do nepopolnih in zato tudi neučinkovitih rešitev.
- ***Preprostost načrta***. Zaradi časovne stiske in drugih pritiskov pri okrevalnem postopku je možnost neuspeha pri zapletenih in obsežnih okrevalnih načrtih večja kakor pri preprostejših.

- ***Trajno vzdrževanje***. Izvajanje okrevalnih ukrepov ni enkratna naloga, pač pa mora postati stalnica pri oblikovanju informacijskega sistema pa tudi pri načrtovanju razvoja na drugih področjih delovanja organizacije.
- ***Odgovorna oseba ali skupina***. Pokrivanje tega področja mora biti stalna naloga osebe ali posebne skupine, ki nosi odgovornost za vzdrževanje okrevalnih ukrepov in ima za to tudi vsa potrebna pooblastila.
- ***Kategorizacija kritičnosti***. V okrevalnem načrtu morajo biti različne aplikacije smiselno razdeljene glede na njihovo kritičnost za delovanje organizacije. Kategorizacijo kritičnosti je treba stalno spremljati in jo prilagajati spremembam v poslovanju.

Obstoj okrevalnega načrta seveda ni pogoj za začetek uvajanja ukrepov za zagotavljanje delovanja informacijskega sistema. Mnoge organizacije uvajajo take ukrepe tudi brez izdelanega formalnega okrevalnega načrta, če ne upoštevamo dejstva, da se pri uvajanju kakršnih koli ukrepov vedno pojavijo tudi navodila in procedure za njihovo izvajanje, ki skupaj pravzaprav že tvorijo zasnovo okrevalnega načrta. Tak način uvajanja okrevalnih ukrepov je lahko nekaj časa učinkovit, vendar se z njim lahko vzpostavi le delovanje posameznih, navadno ločenih segmentov poslovnega sistema, in zato ne more učinkovito zagotoviti nadaljevanja poslovanja organizacije. Izdelava popolnejšega okrevalnega načrta tako slej ko prej postane nujnost.

4.3 Značilnosti okrevalnih postopkov

Osrednji in najpomembnejši del okrevalnega načrta je, ne glede na izbiro metodologije, namenjen obravnavi postopkov ponovne vzpostavitve delovanja informacijskega sistema organizacije. Pri tem je treba nameniti pozornost trem glavnim elementom sistema: podatkom, kamor sodi tudi programska oprema, strojni opremi in telekomunikacijskim povezavam. Obstaja mnogo načinov ponovnega vzpostavljanja informacijskega sistema, ki se med sabo razlikujejo po kompleksnosti, učinkovitosti in seveda ceni.

Že pri analizi vpliva na poslovanje smo opredelili dve temeljni merili, ki opisujeta zahteve, ki jih morajo zagotoviti okrevalni ukrepi za vzpostavitev poslovnih aplikacij, to sta ciljna točka restavriranja podatkov (RPO) in ciljni čas vzpostavitve delovanja (RTO). Za lažje razvrščanje okrevalnih postopkov glede na ti dve merili je bila na konferenci SHARE User Group leta 1992 v Anaheimu predlagana sedemstopenjska lestvica, ki na enostaven način ponazarja celotni možni spekter spleta okrevalnih postopkov. Kljub temu da je ta razdelitev že dokaj stara, je še vedno uporabna za razvrstitev organizacij glede na vsebino njihovih okrevalnih načrtov, pa tudi za razvrstitev različnih aplikacij in poslovnih procesov v sami organizaciji. V nadaljevanju so prikazane značilnosti različnih okrevalnih rešitev, ki si sledijo glede na ceno njihove implementacije od najcenejše do najdražje (Tate et al., 2002, str. 44–48).

- ***Stopnja 0 – ni okrevalnega načrta***. Organizacija nima nikakršnega okrevalnega načrta, zato so ob nesreči podatki najverjetneje izgubljeni in ni možnosti za ponovno vzpostavitev poslovanja. Taka rešitev seveda ne prinaša nikakršnih stroškov.
- ***Stopnja 1 – kopiranje podatkov***. Podatki in programska oprema se v določenih časovnih presledkih kopirajo na trakove in odvažajo na varno lokacijo. Ob nesreči je treba poiskati nadomestno lokacijo in strojno opremo, vzpostaviti telekomunikacijske povezave in sistem ter restavrirati podatke. Podatki od zadnje kopije do trenutka nesreče so izgubljeni. Stroške take rešitve tvorijo stroški kopiranja na trakove ter stroški prevoza in skladiščenja trakov na oddaljeni lokaciji.
- ***Stopnja 2 – stopnja 1 in zagotovljena lokacija***. Podoben način kopiranja kot pri stopnji 1, le da ima organizacija zagotovljeno in opremljeno nadomestno lokacijo (*Cold Site*). Čas vzpostavitve poslovanja se v primerjavi s prejšnjo stopnjo skrajša, stroški pa se povečajo za stroške vzdrževanja ali najema nadomestne lokacije.
- ***Stopnja 3 – elektronski prenos podatkov***. Podobno kot stopnja 2, le da ima organizacija na oddaljeni lokaciji na razpolago tračni sistem, na katerega kopira podatke po elektronski poti. Čas za vzpostavitev poslovanja se nekoliko skrajša, stroški pa se povečajo za ceno vzdrževanja dodatnega tračnega sistema in ceno občasnega prenosa podatkov med lokacijama.
- ***Stopnja 4 – aktivna sekundarna lokacija***. Poleg rednega kopiranja podatkov se na sekundarno lokacijo asinhrono prenašajo tudi vse vmesne spremembe podatkov (*Warm Site*). S tem načinom se količina izgubljenih podatkov bistveno zmanjša. Stroški rešitve se v primerjavi s prejšnjo stopnjo povečajo za stroške stalne telekomunikacijske povezave, sistema za sprejemanje sprememb in ekvivalentnega diskovnega podsistema na sekundarni strani.
- ***Stopnja 5 – dvofazno potrjevanje podatkov***. Postavitev obeh sistemov je podobna kot pri prejšnji stopnji, le da so aplikacije prilagojene tako, da se podatki zapisujejo in potrjujejo hkrati na obeh straneh. Telekomunikacijske zahteve take povezave so večje, kot pri asinhroni povezavie, zato se pri taki rešitvi povečajo tudi telekomunikacijski stroški.
- ***Stopnja 6 – popolna redundantna sistema***. Organizacija ima na razpolago delujoč sekundarni sistem, ki vsebuje zrcalno sliko vseh podatkov in programske opreme ter je telekomunikacijsko povezano z uporabniki (*Hot Site*). Stroški se povečajo za stroške vzdrževanja delujočega sekundarnega sistema.

V tabeli 5 je prikazan pregled sedmih stopenj okrevalnih postopkov s podatki o potencialni izgubi podatkov in tipičnem času vzpostavitve delovanja. Prikazani so tudi deleži organizacij, ki se po ocenah IBM iz leta 1998 s svojimi okrevalnimi načrti nahajajo na posameznih stopnjah (GDPS: the S/390 Multi-site Application Availability Solution, 1998). V Sloveniji se večina organizacij, vključno s policijo, nahaja na prvi stopnji, izjema se nekatere banke, ki imajo nameščene oddaljene pomnilniške zmogljivosti in se tako nahajajo na tretji stopnji.

Stopnja	Izguba podatkov	Čas vzpostavitve delovanja	Delež organizacij
0	-	-	< 0,3 %
1	24–48 ur	> 48 ur	< 0,1 %
2	24–48 ur	24 ur	90 %
3	< 24 ur	< 24 ur	6 %
4	nekaj minut	< 2 uri	< 0,5 %
5	nekaj sekund	< 2 uri	< 0,1 %
6	0–nekaj sekund	0–nekaj minut	3 %

Tabela 5: RPO, RTO in delež organizacij po posameznih stopnjah okrevalnih postopkov (Vir: IBM, 1998)

V okrevalnem načrtu morajo biti predvideni tudi postopki vračanja na normalno delovanje, na kar se prepogosto pozablja. Ne glede na izbiro tehnologije delovanja alternativnega sistema je treba predvideti tudi postopke ponovne sinhronizacije primarnega informacijskega sistema s spremembami, ki so nastale med delovanjem na alternativnem sistemu. V okrevalnem načrtu je treba načrtovati postopke vračanja na normalno delovanje le za primere začasnega in delnega uničenja oziroma okvare na primarni strani, medtem ko obravnava rekonstrukcije ali nadomestitve primarne lokacije v primerih njenega trajnega in popolnega uničenja ne sodi v okvir okrevalnega načrta.

V nadaljevanju bodo nekoliko podrobneje obravnavani nekateri najpomembnejši elementi, ki sodijo pretežno v tehnični del okrevalnega načrta. To so postopki restavriranja podatkov in programske opreme, postopki restavriranja strojne opreme oziroma vzpostavitev ustreznega nadomestnega sistema za izvajanje ključnih poslovnih aplikacij ter postopki restavriranja telekomunikacijskih povezav. V poglavju 4.7 bodo na kratko prikazani še nekateri drugi, predvsem organizacijski postopki, ki jih mora poleg tehničnih vsebovati okrevalni načrt.

4.4 Restavriranje podatkov in programske opreme

Podatki pomenijo osrednjo točko vsakega informacijskega sistema in njihovo varovanje pred uničenjem je nedvomno najpomembnejša in najodgovornejša naloga njegovih skrbnikov. V podatkih se ohranja zgodovina delovanja organizacije, potrebni so pri njeni vsakodnevni dejavnosti, zaradi vedno večje analitične vrednosti pa postajajo vse pomembnejši tudi pri načrtovanju usmeritev in razvoja organizacije v prihodnje.

V informacijskem sistemu organizacije se nahaja vrsta elektronsko shranjenih podatkov, kot so:

- operativni podatki in dokumenti,
- podatki, potrebni za delovanje sistema (sistemske nastavitve, gesla ipd.),
- strojne programske kode,
- izvorne programske kode,
- notranji podatki in dokumentacija ter elektronska korespondenca,
- arhivski podatki in dokumentacija ipd.

V večini primerov se razmišljanje ustavi pri operativnih podatkih in včasih še pri notranji dokumentaciji, vendar je pri varovanju treba nameniti pozornost prav vsem vrstam podatkov. Za vsakodnevno delovanje sistema in poslovanje organizacije so neposredno potrebne prve tri vrste podatkov, brez katerih informacijski sistem ne more delovati. Zato je te podatke treba varovati v taki obliki, da jih je mogoče obnoviti v najkrajšem možnem času.

Druge vrste podatkov neposredno za delo uporabnikov niso tako pomembne, se pa v njih nahajata znanje in zgodovina organizacije, zato si brez teh vrst podatkov poslovanja na daljši rok ni mogoče predstavljati. Tudi te podatke je zato treba skrbno varovati, le da je na splošno čas njihove restavracije lahko nekaj daljši.

Velika večina organizacij na ta ali oni način varuje vsaj del svojih podatkov v informacijskem sistemu pred izgubo, četudi pri tem morda tudi ne razmišljajo neposredno o zagotavljanju poslovanja. Obstaja mnogo različnih načinov varovanja podatkov, ki so odvisni od velikosti organizacije, količine podatkov, tehnološke platforme informacijskega sistema, splošne varnostne politike v organizaciji ipd.. Na splošno pa se različne metode varovanja podatkov med sabo razlikujejo v treh temeljnih karakteristikah, in sicer glede na vrsto nevarnosti, pred katerimi ščitijo podatke, glede na obseg varovanih podatkov in glede na hitrost obnovitve varovanih podatkov.

4.4.1 Načini zaščite podatkov

Najpreprostejša zaščita podatkov je že njihovo hranjenje na redundantnih tipih podatkovnih nosilcev. Modeli RAID (*Redundant Array of Independent Disks*) diskovnih podatkovnih nosilcev poleg drugih prednosti dajejo tudi odlično zaščito pred okvarami samih podatkovnih nosilcev. Obstaja več različnih metod RAID, ki se med sabo razlikujejo v načinu shranjevanja in kopiranja podatkov, skupna značilnost vseh pa je, da se vsak podatek, ki se nahaja na okvarjenem disku, da restavrirati iz podatkov na drugih diskih v isti skupini. Obnovitev podatkov je takojšnja in za uporabnika neopazna. Tovrstno varovanje je namenjeno predvsem zaščiti pred strojnimi okvarami posameznega diskovnega pogona, ne more pa zagotoviti varovanja podatkov ob okvari ali uničenju celotnega diskovnega sistema.

Nekoliko boljšo zaščito zato daje redno kopiranje podatkov na trakove ali drug diskovni sistem ter vodenje dnevnika sprememb na operativnih podatkih. Poglavitni namen rednega kopiranja je predvsem možnost hitrega restavriranja podatkov ob okvari podatkovnega nosilca, na katerem se podatki nahajajo, zato morajo biti kopije in dnevniki blizu in hitro na razpolago. Kopiranje ponuja možnost restavriranja podatkov ob okvari celotnega diskovnega podsistema ali ob logični okvari podatkov zaradi napake v aplikaciji. Ker se morajo kopije zaradi potrebe po čim krajšem času restavriranja nahajati blizu, najbolje v računalniškem centru, ta rešitev ne zagotavlja varstva pred nesrečami, ki prizadenejo celotni center, kot sta na primer požar ali poplava.

Da bi zagotovili možnost restavriranja podatkov ob nesreči večjih razsežnosti, pa je treba kopije podatkov shranjevati tudi na oddaljeni lokaciji. Obstaja več tehnik, s katerimi je mogoče to doseči in ki se med sabo razlikujejo po ceni izvedbe ter po ažurnosti kopiranih podatkov. V nadaljevanju so navedeni trije možni načini kopiranja podatkov na oddaljeno lokacijo s kratkim opisom njihovih glavnih značilnosti:

- ***Kopiranje na trakove in odvažanje trakov na varno lokacijo***. Najstarejša in najcenejša tehnika, ki se še vedno najpogosteje uporablja. Ažurnost podatkov je odvisna od pogostnosti kopiranja in odvažanja trakov, ki se odvija v najboljšem primeru enkrat na dan, navadno pa še redkeje. Dobra stran tega načina je nizka cena, slabi strani pa sta predvsem možnost napak zaradi ročnega posredovanja in dolgotrajno restavriranje podatkov. Zaradi hitre rasti količine podatkov se v organizacijah, ki poslujejo v režimu 24 x 7, lahko pojavita tudi problema določanja točke konsistentnosti in pomanjkanja časa za kopiranje podatkov.

- ***Kopiranje na oddaljeni tračni sistem***. Ta način kopiranja je dražji od prejšnjega, saj zahteva vzdrževanje dveh tračnih sistemov, oddaljene lokacije in telekomunikacijske povezave med njima. Zagotavlja precej večjo ažurnost podatkov, saj je mogoče kopirati podatke pogosteje, lahko se kopirajo dnevniki sprememb in delajo inkrementalne kopije, poleg tega je zaradi avtomatizacije postopka možnost napak bistveno manjša. Še vedno pa ostaja problem dolgotrajnega restavriranja podatkov s trakov.

- ***Kopiranje podatkov na oddaljeni diskovni sistem***. Najdražji način kopiranja podatkov, ki terja vzdrževanje dveh diskovnih sistemov in precej zmogljivo medsebojno povezavo. Podatki se lahko kopirajo sinhrono – podatki se spreminjajo sočasno na obeh diskovnih sistemih, ali asinhrono – podatki na oddaljenem diskovnem sistemu se spreminjajo z zamudo, ki navadno traja od nekaj sekund do nekaj minut. Ker se podatki na oddaljeni lokaciji nahajajo v izvorni obliki, so po potrebi lahko takoj na razpolago oziroma jih ni treba posebej restavrirati.

4.4.2 Kopiranje podatkov na oddaljeni diskovni sistem

V zadnjih letih se vsaj v večjih organizacijah čedalje pogosteje uporablja metoda kopiranja podatkov na oddaljeni diskovni sistem. Vzroki za to so predvsem trije. Prvi vzrok je vedno večja potreba po zagotavljanju popolne ali skoraj popolne možnosti obnovitve podatkov, kar lahko zadovoljivo omogoči le metoda replikacije podatkov. Drugi pomembni razlog je v čedalje bolj razširjenem načinu poslovanja 24 x 7, zaradi česar ni več na razpolago dovolj časa niti za kopiranje podatkov niti za morebitno restavriranje podatkov s tračnih medijev. Tretji in verjetno odločilni vzrok za to pa je iskati v bistveni pocenitvi diskovnega pomnilniškega prostora v zadnjih letih, saj se je na primer nabavna cena prostora na disku v zadnjih petih letih zmanjšala za približno 90 odstotkov, pri čemer cene padajo še naprej.

Obstajata dva bistvena načina kopiranja podatkov na oddaljeni diskovni sistem – asinhroni in sinhroni, poleg tega pa se pojavljajo še nekatere kombinacije obeh načinov. Kronološko starejši je asinhroni način kopiranja, kjer se spremembe podatkov na primarnem sistemu zbirajo in z določeno časovno zamudo v paketu pošiljajo na sekundarno stran. Slika podatkov na sekundarni strani pri tem načinu tako zaostaja za stanjem na primarni strani, kar je tudi glavna pomanjkljivost tega načina v primerjavi s sinhronim. Zaostanek je odvisen predvsem od intenzivnosti sprememb podatkov na primarni strani, delno pa tudi od kakovostne medsebojne povezave in je navadno dolg od nekaj sekund v času nizke do nekaj minut v času visoke intenzivnosti sprememb.

Sinhroni način kopiranja temelji na principu dvojnega potrjevanja, kar pomeni, da sprememba podatka na primarnem diskovnem sistemu ni izvedena, dokler ni potrjena še s sekundarne strani. Na ta način je doseženo, da je slika podatkov na sekundarni strani v vsakem trenutku enaka stanju podatkov na primarni strani, čeprav vendarle obstaja tudi majhna teoretična možnost, da pride do neskladij med obema stranema. Primerjava obeh metod je prikazana v tabeli 6.

Dodatne primerjave obeh načinov kopiranja v različnih strojnih okoljih je mogoče dobiti v literaturi (primer Scott, Krischer, Rubin, 2001). Pred izbiro načina kopiranja podatkov je treba proučiti prednosti in slabosti obeh načinov ter jih primerjati s potrebami in konfiguracijo informacijskega sistema v organizaciji.

Glede na to, da ima vsaka od metod varovanja podatkov svoje prednosti in slabosti, lahko postavimo trditev, da se te metode med sabo ne izključujejo, pač pa dopolnjujejo. Zato se pri postopkih za zagotavljanje delovanja informacijskega sistema ne postavlja vprašanje, katera od teh metod je najprimernejša za varovanje podatkov v organizaciji, pač pa katere podatke varovati s posamezno metodo. Da bi lahko odgovorili na to vprašanje, je treba podatke razvrstiti glede na njihovo pomembnost za organizacijo in potrebno ažurnost ter na podlagi te razvrstitve določiti za posamezne kategorije podatkov ustrezni način varovanja.

	asinhroni način	***sinhroni način***
Izguba podatkov	*do nekaj minut*	*nič do nekaj sekund*
način medsebojne povezave	*optično vlakno ali komercialna povezava*	*optično vlakno*
zmogljivost medsebojne povezave	*zmerna*	*velika*
medsebojna oddaljenost	*neomejena*	*največ 100 km vlakna*
vpliv na odzivni čas	*ga ni*	*precejšen, narašča z oddaljenostjo*
lastnosti diskovnih sistemov	*sistema sta lahko različna, tudi od različnih proizvajalcev*	*sistema morata biti identična*
odpornost na stopnjujoče se nesreče (*rolling disasters*)	*da*	*da*

Tabela 6: Primerjava asinhronega in sinhronega načina kopiranja podatkov med dvema diskovnima sistemoma

4.4.3 Razvrstitev podatkov

Narava podatkov v različnih organizacijah je zelo različna, zato je težko opredeliti splošna pravila, kako naj se podatki razvrstijo. Pri tem postopku je najprej treba evidentirati vse relevantne podatke, ki se nahajajo v informacijskem sistemu organizacije, pri čemer je treba:

- določiti vse podatke in dokumente, ki so nujno potrebni za vzpostavitev minimalnega vsakodnevnega delovnega procesa v organizaciji,
- določiti podatke, ki so potrebni za vzpostavitev poslovanja v celotnem obsegu,
- določiti podatke, ki jih mora organizacija hraniti zaradi predpisov in zakonskih razlogov.

Potem ko so evidentirani vsi relevantni podatki, jih je treba razvrstiti glede na stopnjo njihove kritičnosti za organizacijo in s tem nujnosti njihovega varovanja. Toigo predlaga preprosto štiristopenjsko klasifikacijsko lestvico, ki je prikazana v tabeli 7 (Toigo, 2000, str. 118).

Poleg pomena posameznih vrst podatkov je za zagotavljanje poslovanja zelo pomemben tudi čas, v katerem je posamezne vrste varovanih podatkov mogoče obnoviti. Zato je pri razvrstitvi podatkov treba izhajati iz ugotovitev analize vpliva na poslovanje in izbrati za kritične podatke tako metodo kopiranja, ki omogoča obnovitev ali dostop do podatkov v času, ki je krajši od največjega dopustnega časa prekinitve poslovanja. Za podatke nižjih stopenj kritičnosti, katerih takojšnja razpoložljivost ni tako nujna za zagotovitev poslovanja, je

smotrno izbrati cenejše metode varovanja, pri katerih pa je čas dostopa do podatkov nekaj daljši.

Stopnja	***Opis***
Kritični	*Podatki, ki so nujno potrebni za zagotovitev minimalnega vsakodnevnega poslovanja organizacije, kot so vhodni in izhodni operativni podatki, podatki, potrebni za delovanje sistema in programske strojne kode.* *V to skupino sodijo tudi podatki in dokumentacija, ki jih mora organizacija varovati zaradi zakonskih predpisov.* *Kritične podatke je treba varovati z največjo zanesljivostjo. Treba je hraniti več kopij na različnih lokacijah, pri čemer je najbolje uporabiti različne metode kopiranja, če so v organizaciji na razpolago.*
Vitalni	*Podatki in dokumentacija, ki so potrebni za popolno obnovitev normalnega poslovanja organizacije in jih ni mogoče obnoviti iz drugih virov. V to skupino sodijo na primer interni podatki, analize, organizacijski know-how, razvite izvorne programske kode ipd.* *Te podatke je treba varovati s podobno visoko zanesljivostjo, kot to velja za kritične podatke, le število varnostnih kopij je lahko manjše.*
Občutljivi	*Podatki, ki so potrebni za vzpostavitev normalnega poslovanja, vendar jih je mogoče kolikor toliko učinkovito obnoviti tudi iz alternativnih virov, kot so na primer skladišča podatkov, kupljena programska oprema ipd.* *Občutljivih podatkov ni treba varovati z več kot eno kopijo, pri čemer je smotrno uporabiti cenejše metode varovanja.*
Nekritični	*Podatki in dokumentacija, ki za zagotavljanje poslovanja niso neposredno potrebni ali pa jih je mogoče brez težav obnoviti tudi iz alternativnih virov.* *Te podatke je smotrno varovati le z najpreprostejšimi in najcenejšimi metodami, lahko pa ostanejo tudi brez posebnega varovanja, saj njihovo morebitno uničenje ne vpliva na poslovanje organizacije ali pa je vpliv minimalen.*

Tabela 7: Klasifikacijska lestvica kritičnosti posameznih vrst podatkov v organizaciji (Vir: Toigo, 2000)

4.4.4 Varovanje distribuiranih podatkov

Posebno problematični za varovanje so podatki, ki so fizično razpršeni, kot so na primer distribuirane baze podatkov ali sistemske nastavitve distribuiranih strežnikov. Varovanje tovrstnih podatkov je v praksi največkrat prepuščeno lokalnim administratorjem ali celo končnim uporabnikom. V obeh primerih je zelo težko uveljaviti primerno metodo in standarde varovanja podatkov, saj je izvajanje varovalne politike praktično nemogoče nadzorovati. Prav zato v zadnjih letih čedalje več organizacij, predvsem večjih, v svojih informacijskih sistemih vpeljuje tako ali drugačno obliko koncentracije virov. Pri tem se

odločajo bodisi za koncentracijo strežnikov, o čemer več pozneje, bodisi za koncentracijo podatkov.

Podatke je mogoče koncentrirati na logični ravni, kar pomeni, da se razpršene baze podatkov združijo v eno, centralno nadzirano bazo. Tak reinženiring je sicer mogoče narediti, če se uporablja enak sistem za upravljanje baz na distribuiranih strežnikih, vendar je tudi v tem primeru to zelo zapleten in dolgotrajen postopek, ki zahteva vrsto prilagoditev in sprememb na baznih objektih. V organizacijah se zato raje odločajo za fizično koncentracijo podatkov v okviru ene od mrežnih topologij za podatkovne nosilce (*Storage Area Network – SAN* ali *Network Attached Storage – NAS*). To še posebej velja, če uporabljajo raznovrstne podatkovne in strežniške sisteme. Ne glede na uporabljeno tehnologijo je tako koncentrirane podatke bistveno lažje in ceneje kopirati ter pozneje obnoviti, kot je to mogoče narediti z distribuiranimi podatki.

4.4.5 Varovanje podatkov, ki niso v elektronski obliki

Seveda pa organizacije ne razpolagajo le s podatki v informacijskem sistemu, saj je izjemno veliko organizacijskega znanja shranjenega v drugačni obliki, na primer na papirju ali na mikrofilmih. Po nekaterih podatkih naj bi se delež takih, nestrukturiranih podatkov gibal celo okrog 90 odstotkov (Toigo, 2000, str. 115), zato je treba hkrati s sistemom varovanja elektronskih podatkov poskrbeti tudi za sistem varovanja nestrukturiranih podatkov, na kar se rado pozablja.

Tovrstne podatke je mogoče varovati s fizičnim kopiranjem in shranjevanjem kopij na različnih lokacijah ali z digitaliziranjem in shranjevanjem ter varovanjem podatkov v elektronski obliki. Gartner priporoča uporabo obeh načinov varovanja, saj je fizično kopiranje potrebno predvsem zaradi zakonskih razlogov, medtem ko digitalizirana dokumentacija poleg lažjega in cenejšega varovanja prinaša še dodatne koristi zaradi širše dostopnosti (Logan, 2002).

Ker gre za zelo velike količine podatkov, je treba pred digitalizacijo dokumente razvrstiti in izbrati le tiste, ki so pomembni za zagotavljanje poslovanja, kot so na primer računi, pogodbe, računovodski podatki ipd. Poleg tega se je treba tudi odločiti o načinu shranjevanja digitaliziranih podatkov, saj je na trgu na razpolago precej različnih programskih produktov in pomnilniških medijev, ki jih je mogoče uporabiti (Calvert, 2002).

4.4.6 Varovanje podatkov na oddaljeni lokaciji

Varovanje podatkov na način, ki zagotavlja delovanje informacijskega sistema in nadaljevanje poslovanja organizacije tudi ob večjih nesrečah, zahteva, ne glede na izbiro metodologije,

shranjevanje kopije podatkov na oddaljeni lokaciji. Pri tem se je treba v organizaciji odločiti, na kakšen način bi bilo to rešitev treba izpeljati, da bi bila tehnično, varnostno in ekonomsko najbolj učinkovita. Na voljo so naslednje tri možnosti, kot si sledijo od najcenejše do najdražje:

- ***Recipročni dogovor***. Organizaciji, ki imata podobno konfigurirana informacijska sistema in razpolagata s primernimi zmogljivostmi, se lahko dogovorita za medsebojno izmenjavo virov, na primer pomnilniških, telekomunikacijskih ali procesorskih zmogljivosti. Gre za cenovno najugodnejšo možnost, saj se obe strani izogneta stroškom nabave dodatnih zmogljivosti, poleg tega si storitve medsebojno ne zaračunavata. Slaba stran tega načina je predvsem problem zagotavljanja dolgoročnosti medsebojnega dogovora. Velika verjetnost je namreč, da bosta organizaciji zaradi različnih strateških interesov, razvojnih ali tehnoloških strategij ipd., slej ko prej prisiljeni razdreti sklenjeni dogovor in s tem ogroziti varnost svojih informacijskih sistemov, kar je tudi razlog, da se po svetu v zadnjih letih ta možnost precej manj uporablja (Mingay, 2002). Vendar pa za nekatere vrste organizacij, kot so na primer nekatere javne ali državne institucije, kjer navedene slabosti niso tako izrazite, način recipročnega zagotavljanja redundantnih zmogljivosti še vedno lahko velja kot najboljša izbira. V Sloveniji je nekaj primerov velikih državnih in zasebnih organizacij, ki imajo na ta način sklenjene medsebojne dogovore o zagotavljanju zmogljivosti.

- ***Zunanji ponudnik***. Projekt je mogoče deloma ali v celoti opraviti s pomočjo zunanjega ponudnika. Večina večjih svetovnih proizvajalk računalniške strojne opreme, poleg njih pa tudi več neodvisnih specializiranih družb, ponuja možnost varovanja podatkov bodisi kot zaključen projekt bodisi kot najem zmogljivosti ali svetovalno storitev. Prednosti take rešitve so v tem, da ni visokih začetnih stroškov, povezanih z nakupom redundantnih zmogljivosti, da ni treba najemati in izobraževati dodatnega kadra ter da je mogoče celotno rešitev relativno hitro realizirati. V zahodnih državah se ta rešitev veliko uporablja, pri nas pa razen svetovanja ponudniki za zdaj še ne ponujajo tovrstnih rešitev, vsaj ne za večje organizacije.

- ***Lastna rešitev***. Organizacija sama opremi oddaljeno lokacijo in skrbi za kopiranje podatkov s svojimi zmogljivostmi. Ta rešitev je od vseh najdražja in terja največ časa za uresničitev, saj je treba opremiti lokacijo, nabaviti vso potrebo opremo, vzpostaviti telekomunikacijske povezave in izšolati lastni kader, ki bo skrbel za pravilno delovanje. Prednost te rešitve je predvsem v tem, da lahko organizacija postavi in vzdržuje natančno takšne varnostne standarde, kot jih potrebuje, in da v celoti odloča o vseh elementih postavljenega sistema. Rešitev je mogoče deloma poceniti s tem, da se projekta skupaj loti več organizacij s podobnimi varnostnimi zahtevami in informacijskimi sistemi, vendar je v tem primeru najverjetneje treba sprejeti nekatere

kompromise, s čimer pa se poveča tveganost projekta. V Sloveniji je nekaj večjih organizacij, predvsem s področja bančništva, ki uporabljajo tako rešitev.

4.4.7 Varovanje podatkov v slovenski policiji

Slovenska policija varuje svoje podatke, ki se nahajajo na centralnem računalniškem sistemu, z rednim kopiranjem na trakove, kjer se hrani do pet zaporednih kopij podatkov, in s hranjenjem podatkov na redundantnih diskovnih zmogljivostih (RAID). Za varovanje podatkov v primeru uničenja celotnega računalniškega centra se v rednih presledkih kopirajo vsi podatki centralnega pomnilniškega sistema na trakove, ki se odnašajo na varno lokacijo.

Pogostnost kopiranja je odvisna od narave podatkov in se giblje od enega tedna za operativne podatke do tri mesece za izvirne programske kode in sistemske nastavitve. Podatki se v podatkovnih bazah kopirajo avtomatizirano z orodji, ki jih za kopiranje podatkov vsebujejo posamezni sistemi za upravljanje baz, zato je zagotovljena konsistentnost in možnost obnovitve na drugem sistemu. Druge vrste podatkov se kopirajo »ročno« na ravni podatkovnih nosilcev.

Ocenjeno je, da je mogoče z načinom varovanja podatkov, ki je trenutno v veljavi, obnoviti podatkovne baze na drugi lokaciji v šestih urah, pri čemer je potencialna izguba posameznih vrst podatkov odvisna od frekvence kopiranja, vendar ni daljša od sedmih dni. Trenutna konfiguracija sistema je takšna, da se na lokalnih strežnikih ne nahajajo pomembnejši operativni podatki, zato je varovanje teh podatkov urejeno na lokalni ravni in zanj skrbijo lokalni administratorji. Podatki na nekaterih strežnikih, ki se nahajajo na osrednji lokaciji, se z namensko programsko opremo kopirajo na centralni diskovni sistem.

Sistem varovanja podatkov slovenske policije znotraj računalniškega centra je v varnostnem, tehničnem in finančnem pogledu povsem zadovoljiv, česar pa ne bi mogli trditi za varovanje podatkov za primer večje nesreče: tako čas obnovitve, kot potencialna izguba podatkov sta pri trenutnem načinu varovanja bistveno predolga. Zahteve Evropske zveze po varovanju zunanje evropske meje držav podpisnic Schengenskega sporazuma, ki ga bo v relativno kratkem času podpisala tudi Slovenija, dovoljujejo največ šesturni izpad informacijske podpore mejnega nadzora. Zahteva po vzpostavitvi delovanja informacijskega sistema v manj kakor šestih urah tudi ob večji nesreči praktično pomeni, da varnostne rešitve, ki predvidevajo obnavljanje operativnih podatkov iz kopij, zaradi predolgega časa obnavljanja niso primerne.

4.4.7.1 Predvidene spremembe

Zato je bila sprejeta odločitev, da se podatki pred izgubo zaradi večje nesreče zavarujejo tako, da se kopirajo na oddaljeni diskovni sistem, kar je bila glede na postavljene zahteve praktično

tudi edina možnost. Izmed obeh metod tovrstnega kopiranja podatkov je bila na podlagi prej navedenih kriterijev izbrana asinhrona metoda, saj so večja varnost zaradi daljše medsebojne razdalje, nižja cena telekomunikacijske povezave med lokacijama in manjši vpliv na odzivne čase transakcij odtehtali nekaj daljši RPO, ki ga ima ta metoda v primerjavi s sinhrono.

Na oddaljeni lokaciji se bo nahajala tudi avtomatska tračna knjižnica, kamor se bodo kopirali podatki, ki se na primarni strani nahajajo na trakovih. Arhivski in statistični podatki na trakovih se bodo kopirali asinhrono, saj obdelave na teh podatkih niso ključnega pomena za policijo, in zato zamude na sekundarni strani niso tako pomembne. Nekoliko težji problem bo s kopiranjem podatkov, ki že dlje časa niso bili uporabljeni in jih operacijski sistem samodejno migrira z diskov na trakove. Za konsistentnost stanja podatkov je izjemno pomembno, da podatki hkrati migrirajo z diskovnih sistemov na obeh lokacijah.

Postopek kopiranja podatkov bo izveden kot del celovite IBM arhitekture GDPS (*Geographically Dispersed Parallel Sysplex*), ki z uporabo serije procedur omogoča avtomatski prenos obremenitve na sekundarni računalniški sistem v primeru načrtovanega ali nepričakovanega izpada primarnega računalniškega sistema. Asinhrono kopiranje podatkov na oddaljeni diskovni sistem bo izvedeno z uporabo topologije IBM XRC (*Extended Remote Copy*), kjer za prenos podatkov skrbi programska oprema na sekundarnem sistemu. Izvedba povezave dveh sistemov v smislu arhitekture GDPS, s tem pa tudi oblikovanje postopkov za kopiranje podatkov med diskovnima sistemoma in tračnima knjižnicama na obeh straneh, bo prepuščena strokovnjakom IBM.

V prvi fazi naj bi se na oddaljeni diskovni sistem kopirali le podatki, ki se nahajajo na centralnem računalniškem sistemu, pozneje pa naj bi se na enak način kopirali tudi podatki z lokalnih strežnikov. Za zdaj še ni bila sprejeta odločitev, na kakšen način naj bi se to izvajalo, razmišljanja pa gredo v dveh smereh. Prva možnost je konsolidacija strežnikov, ki prinaša še nekatere dodatne prednosti, kot bo prikazano pozneje, druga možnost pa je uporaba namenske programske rešitve za kopiranje lokalnih podatkov na centralni diskovni sistem, ki se v omejenem obsegu v slovenski policiji uporablja že zdaj.

4.5 Restavriranje strojne opreme

Restavriranje strojne opreme pomeni ponovno vzpostavitev procesorskih zmogljivosti, s katerimi je mogoče izvajati operacije, ki zagotavljajo informacijsko podporo delovanju poslovnega sistema. Obstaja mnogo načinov vzpostavitve nadomestnih procesorskih zmogljivosti, ki se med sabo tehnološko in finančno lahko zelo razlikujejo, zato je prav izbira načina restavriranja strojne opreme najpomembnejša odločitev, ki jo je pri uvajanju rešitev za zagotovitev poslovanja treba sprejeti. Od te izbire je v marsičem odvisna tudi izbira tehnologije restavriranja podatkov in telekomunikacijskih povezav.

Najprej se je treba odločiti o tem, kateri so tisti ključni poslovni procesi, ki jim je treba zagotoviti informacijsko podporo. Odgovor na to vprašanje izhaja predvsem iz ugotovitev analize vpliva na poslovanje, v tej fazi pa je treba ugotoviti, katere so tiste procesorske zmogljivosti, ki zagotavljajo informacijsko podporo najbolj kritičnim poslovnim procesom. To je mogoče v tehničnem pogledu narediti na več načinov, bodisi z vzpostavitvijo redundantnih strojnih zmogljivosti bodisi z alternativnimi rešitvami, ki emulirajo informacijsko podporo, vendar delujejo z drugačno konfiguracijo strojne opreme. V vsakem primeru pa je treba vzpostaviti tako imenovano minimalno sprejemljivo strojno konfiguracijo, ki je sposobna zagotavljati informacijsko podporo najnujnejšim poslovnim procesom.

Poleg o minimalni konfiguraciji, se je treba odločiti tudi o tem, koliko uporabnikov bo uporabljalo nadomestni sistem. Analiza vpliva na poslovanje daje, vsaj deloma, odgovor tudi na to vprašanje. Pri tem je treba upoštevati, da se število uporabnikov lahko zmanjša le v centrali, saj se podpora dislociranim enotam, kot na primer prodajalnam ali izpostavam, navadno ne da zmanjšati. Število uporabnikov je pomembno predvsem pri restavriranju distribuiranih delov informacijskih sistemov, kjer je poleg same strojne opreme treba zagotoviti tudi druge potrebne delovne razmere.

Podobno kot pri restavriranju podatkov ima tudi pri izbiri načina in možnosti restavriranja procesorskih zmogljivosti zelo pomembno vlogo struktura informacijskega sistema organizacije. Restavriranja strojne opreme distrubuiranega sistema z množico strežnikov v različnih ravneh se je treba lotiti povsem drugače kot restavriranja centraliziranega sistema.

Po eni strani je zagotavljanje delovanja centraliziranega sistema zaradi koncentracije virov in enostavnejšega uvajanja ter nadzora nad varnostnim standardi lažje. Po drugi strani pa so distribuirani sistemi zaradi fizične razpršenosti precej bolj žilavi kot centralizirani, ki zato terjajo mnogo temeljitejše in navadno tudi dražje ukrepe za zagotavljanje delovanja. Vprašanje vpliva konfiguracije informacijskega sistema na možnost zagotavljanja njegovega delovanja ostaja tako odprto. Gartner v svojih analizah ugotavlja, da je s tega stališča najprimernejša centralizirana oblika informacijskega sistema z dvema povezanima centroma (Nicolett, 2001).

Vendar pa danes popolnoma centraliziranih sistemov samo s centralnim računalnikom, kontrolnimi enotami in navadnimi terminalskimi priključki ni praktično nikjer več. Tudi v sistemih z relativno visoko stopnjo centralizacije, kakršen je na primer informacijski sistem slovenske policije, se vsaj del aplikacij izvaja tudi na manjših, namenskih strežnikih. Kljub temu da se na manjših strežnikih pogosto izvajajo manj pomembne aplikacije, je treba za zagotovitev ustrezne informacijske podpore delovanju poslovnega sistema poskrbeti za delovanje nekaterih manjših strežnikov tudi v sicer močno centraliziranih sistemih.

4.5.1 Restavriranje centralnega sistema

Centralno zasnovani informacijski sistemi so tisti, pri katerih se večina aplikacij izvaja na centralnem računalniku kot glavnem podatkovnem in aplikacijskem strežniku. Kljub temu da so lahko tudi nekateri srednji ali manjši sistemi oblikovani centralizirano, se ta pojem navadno uporablja pri večjih sistemih, ki jih poganja bodisi centralni računalnik IBM bodisi kateri od večjih strežnikov Unix izdelovalcev Hewlett-Packard ali Sun. Centralizirani informacijski sistem je zaradi svojih zmogljivosti primeren predvsem za večje organizacije, kjer pa so se najprej začeli ukvarjati s problemom zagotavljanja delovanja svojih informacijskih sistemov, zato so prav pri tovrstnih sistemih pojavile prve tehnike in metode restavriranja procesorskih zmogljivosti.

V nadaljevanju so navedene glavne značilnosti, prednosti in slabosti štirih različnih metod, ki jih uporabljajo organizacije za restavriranje centralnega računalniškega sistema. Sledijo si od najcenejše do najdražje (Toigo, 2000, str 167–178).

4.5.1.1 Restavriranje brez nadomestnih zmogljivosti

Najpreprostejši način restavracije strojne opreme je način brez vnaprejšnje priprave nadomestnih zmogljivosti. Delajo se bolj ali manj ažurne in popolne kopije podatkov, ki so shranjene na varni lokaciji, nadomestne strojne zmogljivosti in telekomunikacijske povezave pa se iščejo šele tedaj, ko so uničene primarne zmogljivosti. V času do ponovne vzpostavitve sistema organizacija ostane brez aktivne informacijske podpore in poslovne operacije opravlja na kak drugačen, alternativni način.

Prednost takega načina je v nizki ceni, saj ne prinaša nikakršnih dodatnih stroškov, vendar pa je tak način restavriranja strojne opreme dolgotrajen in precej tvegan. RTO je od nekaj dni do nekaj tednov, tveganje pa je veliko, saj ni vnaprej jasno, kje bo mogoče dobiti ustrezne nadomestne zmogljivosti. Poleg tega testiranje vzpostavitve sistema ni mogoče, zato obstaja dokaj realna verjetnost, da bodo pri restavriranju sistema nastale težave ali pa se sistema celo ne bo dalo restavrirati, na primer zaradi pomanjkljivih podatkov.

Tveganje glede nadomestnih zmogljivosti je mogoče delno zmanjšati s sklenitvijo vnaprejšnjega dogovora z dobavitelji strojne opreme o pospešeni dobavi opreme in z lastniki primernih prostorov za morebitno postavitev nadomestnega centra. Kljub temu pa pri tej metodi še vedno ostaja problem izjemno dolgega časa vzpostavitve, ki za večino organizacij ne more biti sprejemljiv.

Ne glede na svoje velike pomanjkljivosti pa je ta metoda še vedno najbolj razširjena, v Sloveniji, na primer, jo uporabljajo praktično vse večje organizacije s centraliziranim informacijskim sistemom.

4.5.1.2 »Cold Site«

Organizacija ima na razpolago primerne nadomestne prostore in strojne zmogljivosti, ki pa so v mirovanju. Po potrebi se s z uporabo kopij podatkov naloži in konfigurira operacijski sistem in sistemska programska oprema, restavrirajo baze podatkov ter vzpostavijo telekomunikacijske povezave med nadomestnim centrom in uporabniki.

Ta način restavriranja strojnih zmogljivosti je precej dražji v primerjavi s prejšnjim zaradi stroškov vzdrževanja nadomestne lokacije, opreme in telekomunikacijskih povezav, vendar pa se s tem bistveno zmanjša tveganje, saj so nadomestne zmogljivosti na razpolago, poleg tega je omogočeno tudi redno testiranje vzpostavitve rezervnega sistema. Povprečni čas vzpostavitve pri tej metodi je okrog 24 ur, z dobro organizacijo in dobro usposobljeno ekipo strokovnjakov pa ga je mogoče skrajšati še za nekaj ur.

Ker so stroški vzdrževanja nadomestne lokacije relativno visoki, si lahko organizacije, ki uporabljajo tak način restavriranja strojne opreme, pomagajo pri njihovem zniževanju z enim od naslednjih načinov:

- ***Medsebojni dogovor.*** Dve organizaciji s tehnološko enakima in po velikosti podobnima informacijskima sistemoma si lahko s pogodbo ali dogovorom medsebojno odstopita del procesorskih zmogljivosti za potrebe vzpostavitve nadomestnega sistema. Ta način prinaša le stroške vzdrževanja nekoliko povečanih zmogljivosti strojne opreme v obeh organizacijah ter v primeru medsebojnega kopiranja podatkov še stroške medsebojne telekomunikacijske povezave, sicer pa veljajo enake ugotovitve, kot za dogovor dveh organizacij o medsebojnem kopiranju podatkov. Pri dogovarjanju je treba paziti, da imata organizaciji, ki sklepata dogovor, svoja računalniška centra medsebojno dovolj oddaljena, da ni nevarnosti, da bi oba centra prizadela ista nesreča.

- ***Skupni center za več organizacij.*** Več organizacij s podobno strojno opremo lahko vzpostavi, opremi in vzdržuje skupno nadomestno lokacijo, s čemer se sorazmerno zmanjšajo tudi stroški. Zmogljivost strojne opreme na nadomestni lokaciji je odvisna od dogovora, navadno pa ne presega bistveno potreb največje od pogodbenih organizacij. Dodatna prednost tega načina je v tem, da je s skupno organizacijo ter s skupnimi sredstvi in znanjem mogoče pridobiti vrhunsko nadomestno lokacijo in jo izjemno kakovostno opremiti. Slabost tega načina pa je v tem, da so sodelujoče organizacije zaradi tega prisiljene v sklepanje kompromisov, na primer pri nabavi nove strojne opreme, ki mora biti tipizirana in povsem združljiva z opremo na nadomestni lokaciji. Zaradi tesnega sodelovanja je navadno taka rešitev primernejša za državne in javne institucije kakor za poslovne organizacije. Odličen primer takega sodelovanja obstaja v Avstriji, kjer se je več ministrstev in nekaj javnih organizacij povezalo in vzpostavilo zelo dobro varovan in opremljen nadomestni center v okolici

Salzburga. Po izkušnjah avstrijske policije je mogoče na tej lokaciji vzpostaviti sistem približno v 18 urah.

- ***Zunanji ponudnik.*** Z zunanjim ponudnikom je mogoče skleniti dogovor o najemu rezervnih zmogljivosti, ki se lahko nahajajo na stalni lokaciji pod nadzorom ponudnika ali pa ima ponudnik na voljo mobilni center, ki ga je v dogovorjenem času sposoben pripeljati in konfigurirati v skladu z naročnikovimi zahtevami ter povezati z uporabniki. Pogodba je lahko omejena le na zagotavljanje nadomestnih zmogljivosti, lahko pa predvideva tudi dodatne storitve ponudnika, kot so svetovanje in pomoč pri restavriranju sistema. Taka rešitev je nekaj dražja, zato pa ima organizacija več manevrskega prostora pri izbiri svoje opreme, saj se mora ponudnik v skladu s pogodbo prilagajati spremembam na strani naročnikovega informacijskega sistema. V Sloveniji take rešitve trenutno nihče ne uporablja, po svetu pa je precej razširjena.

4.5.1.3 »Warm Site«

Organizacija ima na voljo nadomestno lokacijo s polno konfigurirano strojno opremo in telekomunikacijskimi povezavami do svojih uporabnikov, pri čemer pa je procesor na nadomestni lokaciji v stanju pripravljenosti in se samodejno zažene le ob načrtovanem ali nenadnem izpadu primarnega sistema. Podatki se stalno kopirajo na sekundarni sistem, bodisi sinhrono bodisi asinhrono. RPO odvisno od izbire tehnike kopiranja podatkov znaša od nekaj sekund do nekaj minut, RTO pa je navadno krajši od dveh ur.

Stroški take postavitve so zelo visoki, saj je poleg vzdrževanja nadomestne lokacije in strojne opreme treba vzdrževati tudi stalno povezavo med primarnim in sekundarnim centrom za prenos podatkov ter povezavo med uporabniki in sekundarnim centrom. Stroške je sicer mogoče nekoliko znižati z dogovorom o skupnem sekundarnem centru z drugimi organizacijami s tehnološko enakimi informacijskimi sistemi, vendar so prihranki relativno majhni. Na ta način namreč ni mogoče pomembneje zmanjšati zmogljivosti nadomestne strojne opreme, stroški vzdrževanja telekomunikacijskih povezav pa ostajajo nespremenjeni.

Ta način restavriranja strojne opreme, ki je tehnološko precej zahteven, se je pojavil v zadnjih nekaj letih in se v svetu zelo hitro uveljavlja. Razlog za to je predvsem v čedalje bolj pogosti potrebi po hitri in avtomatizirani vzpostavitvi nadomestnega informacijskega sistema. V Sloveniji tega načina za zdaj ne uporablja še nobena organizacija.

4.5.1.4 »Hot Site«

»Hot Site«. Organizacija ima na voljo dve lokaciji (lahko tudi več) s popolnoma redundantno strojno opremo, tako da se obremenitev enakomerno razporeja med obema sistemoma. V

primeru izpada enega od obeh sistemov celotno breme prevzame delujoči sistem, ki mora biti za to primerno dimenzioniran, prenos pa je izveden tako, da ga uporabniki v večini primerov sploh ne zaznajo.

Tak način omogoča najvišjo mogočo stopnjo zagotavljanja delovanja sistema, vendar pa so stroški vzdrževanja takega sistema izjemno visoki, saj je treba vzdrževati dve aktivni lokaciji ter zelo obremenjene telekomunikacijske povezave med centroma in največkrat tudi med centroma in uporabniki. Edina slabost take postavitve je v tem, da je zaradi potrebe po zagotavljanju istega časovnega takta na obeh sistemih največja medsebojna razdalja med centroma omejena na nekaj kilometrov, zaradi česar obstaja nevarnost, da oba centra prizadene ista nesreča.

Za zdaj zaradi zelo visokih stroškov tak način uporabljajo le tiste organizacije, ki se ukvarjajo s poslovnimi področji, kjer praktično ne sme priti do izpada, kot so avtorizacije kreditnih kartic in bančništvo. Vendar pa se v zadnjem času zaradi padanja cen strojne opreme in telekomunikacijskih povezav za tako rešitev odloča čedalje več organizacij tudi z drugih področij.

Pri izbiri najprimernejše metode restavriranja strojne opreme mora organizacija izhajati iz ugotovitev analiz tveganja in poslovanja. Ker pa poslovanje postaja čedalje bolj odvisno od informacijske podpore in si organizacije ne morejo več privoščiti dolgotrajnega izpada ali celo tveganja, da sistema ne bodo mogle ponovno vzpostaviti, se čedalje več organizacij odloča za prehod na eno od zadnjih dveh metod restavriranja strojne opreme. Dodatno spodbudo za ta prehod pomenijo tudi v zadnjih letih vztrajno padajoče cene strojne opreme in telekomunikacijskih povezav, zaradi česar so postale bolj kakovostne metode restavriranja cenovno mnogo bolj sprejemljive.

4.5.1.5 Izbira sekundarne lokacije za računalniški center

Pri odločitvi za *Cold Site*, *Warm Site* ali *Hot Site* način restavriranja strojne opreme mora organizacija sama ali v sodelovanju z drugimi organizacijami izbrati stalno oddaljeno lokacijo za namestitev sekundarnega računalniškega centra. Odločitev za izbiro oddaljene lokacije je izjemno pomembna, saj mora ta ustrezati številnim varnostnim in tehničnim zahtevam, poleg tega pa mora biti cenovno kar najbolj ugodna. Ker je vzpostavitev oddaljenega centra relativno drag in tehnično zahteven projekt, je treba izbirati lokacijo zelo pazljivo in pri tem čim bolj upoštevati tudi dolgoročni razvoj informacijskega sistema, saj je že sprejeto odločitev pozneje zelo težko spremeniti.

Pri izbiri oddaljene lokacije je treba izhajati iz dveh izhodišč. Prvo izhodišče so splošna priporočila, ki se nanašajo na varnostne in druge značilnosti, katerim morajo ustrezati izbrana mikrolokacija in prostori za namestitev centra sami po sebi, na primer potresna ogroženost,

infrastrukturna opremljenost ipd. Drugo izhodišče pa sestavljajo značilnosti sekundarne lokacije v razmerju do glavne lokacije, kot sta na primer medsebojna oddaljenost ali infrastrukturna soodvisnost. Vsa splošna priporočila je seveda treba upoštevati v okviru ugotovitev analize tveganja, kjer so opredeljene povsem specifične in konkretne okoliščine in nevarnosti, ki lahko vplivajo na delovanje informacijskega sistema posamezne organizacije.

4.5.1.6 Parametri za izbiro sekundarne lokacije

Pri izbiri geografske mikrolokacije in objekta, v katerem naj bi se nahajal oddaljeni računalniški center, je dobro izhajati iz izkušenj in splošnih priporočil, ki jih je mogoče najti v literaturi. V nadaljevanju je na kratko prikazanih nekaj priporočil, kot jih navaja Gartner (Calvert, 2001).

- ***Značilnosti mikrolokacije***.
  - ***Varnost.*** Lokacija naj se nahaja na področju, kjer ni nevarnosti naravnih nesreč, kot so poplave ali plazovi, ali pa je ta nevarnost minimalna. Prav tako naj ne bi bilo v bližini nevarnih objektov, na primer kemičnih tovarn ipd., ki bi lahko ogrozili delovanje.
  - ***Dostopnost.*** Dobre prometne povezave.
  - ***Infrastruktura.*** Dobre optične povezave, ki jih omogočata vsaj dva različna ponudnika telekomunikacijskih storitev, zanesljiva energetska oskrba.
  - ***Okolje.*** Lokacija nekoliko odmaknjena od stanovanj zaradi hrupa generatorja, dovolj prostora za mogoče poznejše širitve.

- ***Značilnosti objekta.***
  - ***Arhitektura.*** Primerna višina in dimenzije prostorov, dostopnost s tovornjakom zaradi velikih kosov opreme, malo ali nič oken, en sam dostop zaradi varnosti, prostori za pisarne za morebitno dlje časa trajajoče delovanje ipd.
  - ***Oprema.*** Klimatske naprave, generator za pomožno napajanje z zalogo goriva za nekaj dni, protipožarna in protivlomna zaščita, mrežna napeljava znotraj prostorov ipd.
  - ***Telekomunikacije.*** Ločene optične napeljave do različnih telekomunikacijskih ponudnikov.

Seveda je priporočilom lažje slediti, če se organizacija odloči za novogradnjo oddaljenega centra in ima pri izbiri lokacije povsem proste roke. V praksi pa se večkrat pojavlja stanje, ko se za oddaljeni center izbira med objekti, ki so že v lasti organizacije, saj je to cenejša, predvsem pa precej hitrejša rešitev. Tudi v slednjem primeru je treba izbrati lokacijo, ki kar najbolj ustreza gornjim priporočilom, sam objekt pa pozneje s predelavami čim bolj ustrezno prilagoditi. V vsakem primeru pa igrajo zelo pomembno vlogo pri odločitvi za oddaljeno

lokacijo tudi varnostni standardi organizacije in ugotovitve analize tveganja. Če so v teh dokumentih dodatne ali strožje zahteve, jih je seveda pri izbiri in prilagoditvah objektov treba upoštevati.

Vendar pa je treba pri izbiri oddaljene lokacije poleg lastnosti mikrolokacije in objekta upoštevati še nekatere druge pomembne zahteve. Gartner je v svoji analizi opredelil nekaj pravil, o katerih je dobro premisliti pred sprejetjem odločitve o izbiri sekundarne lokacije (Scott, 2001).

- ***Tveganje sočasnega izpada oskrbovanja.*** Pri izbiri lokacije za oddaljeni center je treba paziti na to, da se tveganje sočasnega izpada obeh centrov zaradi istega vzroka kolikor je mogoče zmanjša. Najbolje je, da centra oskrbujejo različni komunalni in telekomunikacijski ponudniki, če pa to ni mogoče, kar precej velja za Slovenijo, pa naj bi bila vsaj na različnih oskrbovalnih vozliščih (na primer energetskih vodih, transformatorjih, centralah ipd.).

- ***Tveganje sočasne nesreče.*** Centra naj bosta dovolj oddaljena, da ju ne more prizadeti ista nesreča večjega obsega. To pomeni, da je treba izbrati oddaljeno lokacijo, ki se ne nahaja na isti geološki prelomnici ali na istem poplavnem področju kot primarna. Po tem pravilu naj bi bila oddaljenost med centroma kar največja, na splošno naj bi, vsekakor to velja za Slovenijo, zadoščala razdalja med 15 in 80 kilometri.

- ***Problem dosegljivosti in transporta.*** Kadar se delovanje informacijskega sistema za dlje časa preseli na oddaljeno lokacijo, mora na tej lokaciji dlje časa delati tudi določen del osebja. Da bi bilo za zaposlene delo v takih primerih manj neprijetno, je treba misliti na to, da centra nista predaleč vsaksebi, tako da bi se zaposleni lahko vsak dan vozili na delo. Ta problem postane še posebno pereč, ko je vzrok izpada večja naravna nesreča, ki lahko prizadene tudi zaposlene. Slednje pomeni dodatno težavo pri zagotavljanju njihove navzočnosti na delovnem mestu, ki je močno oddaljeno od doma. Problem je mogoče rešiti tako, da sta na obeh lokacijah stalni ekipi strokovnjakov, vendar le v primeru, da je sistem postavljen tako, da imata obe ekipi zagotovljeno stalno delo (na primer delujoče razvojno okolje ali »*hot site«* na sekundarni lokaciji). Na splošno pa ima zaradi tega problema prednost manjša razdalja med obema centroma.

- ***Telekomunikacijske zahteve.*** Tehnologija povezave sistemov obeh centrov je zaradi svojih telekomunikacijskih zahtev pomemben dejavnik pri odločitvi o medsebojni oddaljenosti lokacij. Pri izbiri tehnologije sinhronega kopiranja podatkov je oddaljenost omejena na največ sto kilometrov vlakna, pri čemer je treba računati s tem, da odzivni časi transakcij z oddaljenostjo naraščajo. Še hujše zahteve postavlja izbira tehnologije dveh povezanih delujočih sistemov, kjer je medsebojna razdalja

zaradi zagotavljanja skupnega takta omejena na največ 40 kilometrov vlakna. Pri izbiri asinhrone replikacije podatkov načelno ni omejitev glede oddaljenosti centrov.

- ***Cena.*** Cena je zelo pomemben element odločitve in pomeni nekakšno podlago za odločitev o izbiri lokacije. Skozi analizo vpliva na poslovanje vpliva na izbiro RTO in RPO in s tem na način povezave dveh sistemov z vsemi posledicami, ki iz tega izhajajo. Poleg tega igra pomembno vlogo pri izbiri lokacije, saj je pri tej poleg varnostne in tehnološke ustreznosti treba upoštevati tudi cenovno ustreznost.

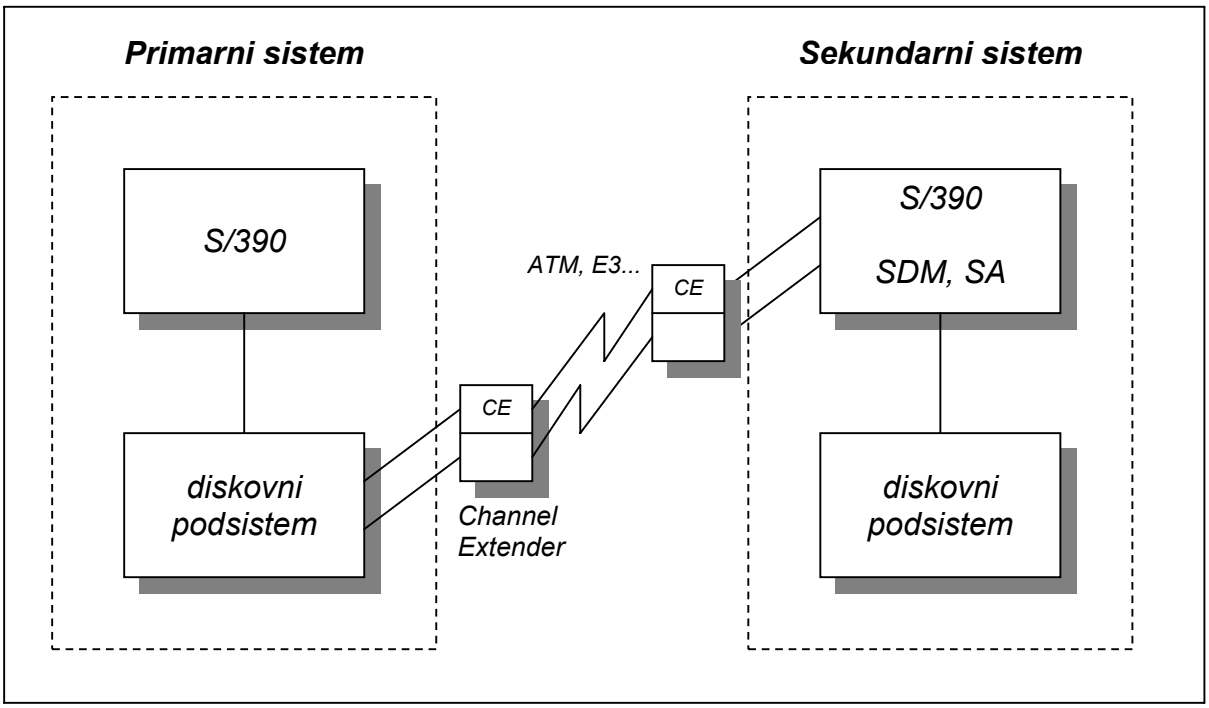
4.5.1.7 Restavriranje centralnega sistema v slovenski policiji

Evropska zveza članicam, podpisnicam Schengenskega sporazuma, katerim se bo kmalu pridružila tudi Slovenija, postavlja jasne zahteve glede zagotavljanja informacijske podpore pri nadzoru evropskih zunanjih meja. Informacijski sistem slovenske policije je zasnovan centralizirano, zato se na centralnem računalniškem sistemu izvaja večina relevantnih aplikacij, med katerimi je tudi informacijska podpora nadzora državne meje, katere del bo v prihodnje postal tudi zunanja meja Evropske zveze. Zaradi centralne zasnove sistema je bila sprejeta logična odločitev, da je prvi korak, ki ga je treba narediti za zagotovitev delovanja informacijskega sistema slovenske policije v skladu z zahtevami Evropske zveze, prav vzpostavitev pogojev za delovanje centralnega računalniškega sistema. Zahteve Evropske zveze so postavljale tudi najostrejši pogoj, ki ga je bilo potrebno pri tem upoštevati.

Zahteva po manj kot šesturnem času vzpostavitve delovanja informacijskega sistema je narekovala tako izbiro načina kopiranja podatkov kot izbiro metode restavriranja strojne opreme. Glede na to zahtevo sta bili sprejeti odločitvi o izbiri asinhronega načina kopiranja podatkov na oddaljeni diskovni sistem in o vzpostavitvi oddaljene lokacije s procesorjem v stanju pripravljenosti, kar pomeni, da je bila izbrana tako imenovana »*Warm Site*« metoda restavriranja. To je najcenejša različica konfiguracije strojne opreme, ki omogoča vzpostavitev delovanja znotraj šesturnega časovnega okvira ob načrtovani in nenačrtovani zaustavitvi primarnega računalniškega sistema.

Sistema na obeh lokacijah bosta med sabo povezana v okviru arhitekture GDPS, s čimer bo omogočen avtomatiziran zagon oddaljenega sistema in prenos obremenitve s pomočjo serije procedur in sistemske programske opreme SA (*System Automation*). Sistem na sekundarni strani je polno konfiguriran in v stanju pripravljenosti, njegova naloga v času mirovanja je omejena na kopiranje podatkov in nadzor delovanja primarnega sistema. Ob načrtovani ali nepričakovani potrebi po zaustavitvi primarnega sistema, sekundarni sistem sproži postopek njegove zamrznitve, polno zažene vse svoje podsisteme, ki so bili v stanju pripravljenosti, vzpostavi povezave z uporabniki in prevzame obremenitev. Čas, ki je potreben za ponovno vzpostavitev delovanja, pri sinhronem načinu kopiranja podatkov znaša od 30 do 60 minut, pri asinhronem načinu pa okrog dve uri. Pregledna skica povezave GDPS dveh računalniških

sistemov z asinhronim kopiranjem podatkov po najetih vodih (GDPS/XRC) je prikazana na sliki 9.



Slika 9: GDPS/XRC povezava dveh centralnih računalniških sistemov

4.5.1.7.1 Izbira lokacije za sekundarni računalniški center slovenske policije

Po odločitvi o zagotavljanju delovanja informacijskega sistema z vzpostavitvijo sekundarnega računalniškega centra je bilo treba izbrati primerno oddaljeno lokacijo. Pri tem je bilo treba izhajati iz priporočil, poleg tega pa upoštevati še posebne varnostne elemente, ki za dejavnosti, kakršna je policijska, še dodatno otežujejo izbiro. Za izbiro lokacije je bila oblikovana posebna ekspertna skupina, ki je bila sestavljena iz strokovnjakov s področij informatike, telekomunikacij in gradbeništva ter varnostnih strokovnjakov.

Ekspertna skupina je pri izbiri oddaljene lokacije izhajala iz dolgoročnih načrtov razvoja policije in upoštevala, da se bodo na tej lokaciji v poznejši fazi poleg računalniškega centra nahajale še nekatere druge vitalne vsebine. Zato je bila sprejeta ocena, da mora objekt na sekundarni lokaciji zagotavljati vsaj 150 kvadratnih metrov stalne uporabne površine višine tri metre ali več v kleti ali pritličju za namestitev naprav, od česar bo 60–80 kvadratnih metrov zasedal računalniški center skupaj s prostorom za operaterje. Poleg tega mora objekt dopuščati tudi možnost za vzpostavitev vsaj 60 kvadratnih metrov pisarn, ki bi jih potrebovali ob daljši selitvi delovanja.

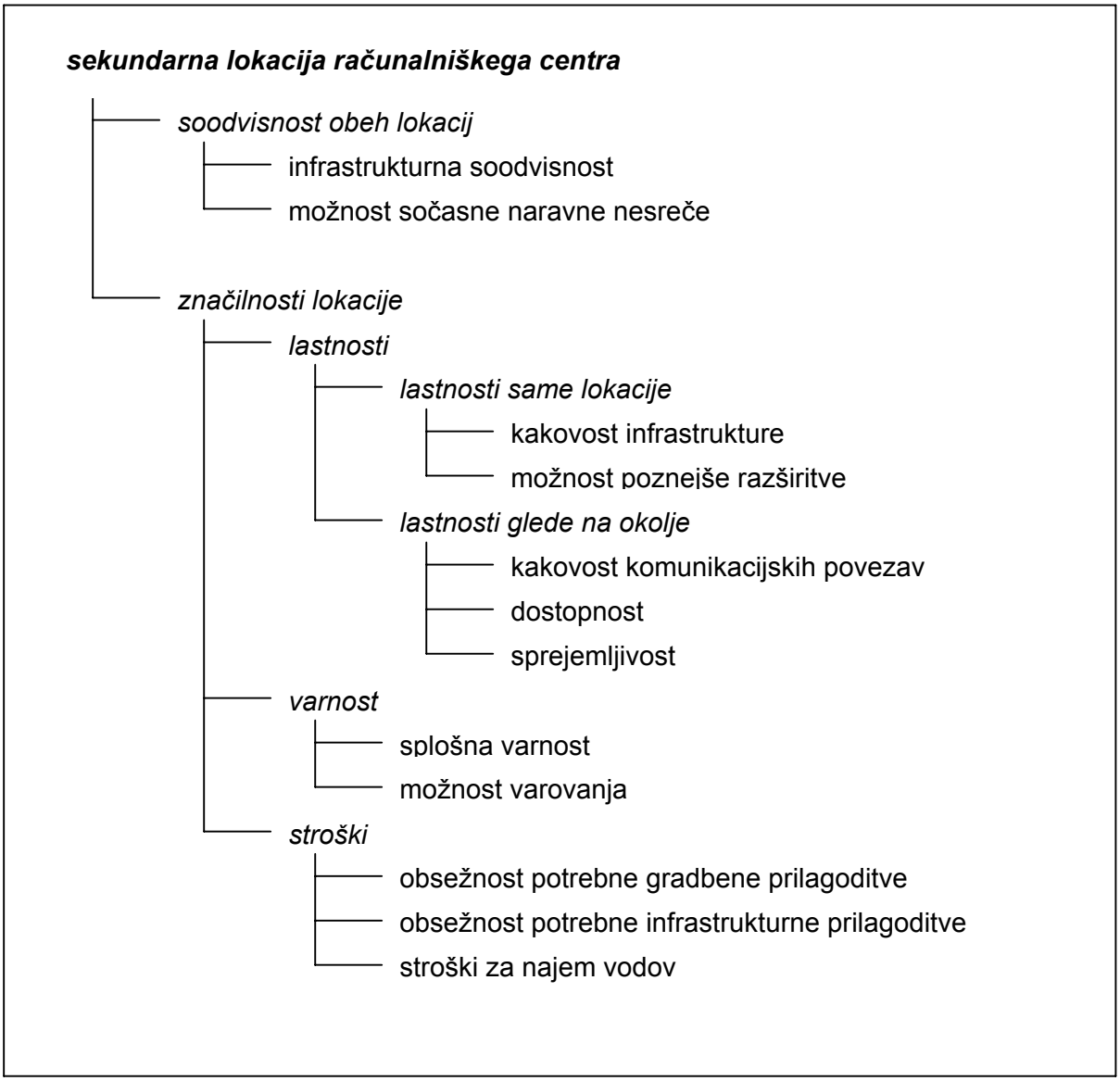
Ker je bilo na razpolago zelo malo časa in ker naj bi bili stroški tega projekta čim manjši, sta bila postavljena še dva kriterija, katerima so morale ustrezati evidentirane potencialne lokacije, in sicer, da je objekt oziroma zemljišče že v lasti policije ter da objekt bodisi ne potrebuje večjih gradbenih posegov za namestitev centra bodisi so gradbeni posegi že predvideni in bi jih bilo treba le deloma prilagoditi.

4.5.1.7.2 Kriteriji za izbiro lokacije sekundarnega računalniškega centra

Na podlagi navedenih prostorskih potreb in ogledov potencialnih lokacij je bilo evidentiranih osem objektov po vsej Sloveniji, ki bi lahko ustrezali za namestitev sekundarnega računalniškega centra. Med temi osmimi objekti je bilo treba izbrati nekaj najbolj primernih, za katere bi se izdelali še študija izvedljivosti in natančnejša varnostna analiza. Zaradi relativno kratkega časa, ki je bil na razpolago, in pomanjkljivih izkušenj se je odločitvena skupina pri izbiri kriterijev in njihovem vrednotenju naslanjala predvsem na napotke iz literature. Na podlagi liste kriterijev je bil izbor najprimernejših objektov narejen z uporabo ekspertnega sistema za podporo večparametrskega odločanja DEXi. Odločitvena skupina je za razvrstitev lokacij opredelila naslednjih 12 kriterijev.

- ***Soodvisnost infrastrukture obeh lokacij.*** Pomembno je, da oba centra (osnovni in rezervni) ne izpadeta hkrati zaradi skupnih energetskih in telekomunikacijskih virov.
- ***Možnost sočasne naravne nesreče.*** Podobno velja, da ista naravna nesreča ne sme hkrati prizadeti obeh centrov.
- ***Kakovost komunikacijskih povezav.*** Lokacija mora imeti možnost priključitve na omrežje vsaj dveh različnih telekomunikacijskih ponudnikov.
- ***Kakovost infrastrukture.*** Kakovost prostorov in gradnje.
- ***Splošna varnost.*** Nevarnost potresa, poplave, oddaljenost od meje ipd.
- ***Možnost varovanja.*** Ali gre za varovano območje, fizično varovanje (ograja, video nadzor ipd.).
- ***Dostopnost.*** Kakovost prometnih povezav, alternativne prometne povezave.
- ***Sprejemljivost.*** Za delavce, ki bodo ob morebitnem daljšem prenosu delovanja morali delati daleč od doma.
- ***Možnost poznejše razširitve.***
- ***Obsežnost potrebne gradbene prilagoditve.*** Novogradnja ali adaptacija.
- ***Obsežnost potrebne infrastrukturne prilagoditve.*** Obstoječe povezave na telekomunikacijsko in energetsko omrežje, klimatske naprave, naprave za neprekinjeno napajanje.
- ***Stroški za najem vodov.***

Nekateri kriteriji opisujejo sorodne značilnosti, zato so bili zaradi lažje obravnave združeni v skupine. Struktura skupin kriterijev in njihova medsebojna odvisnost so prikazane na sliki 10.



Slika 10: Kriteriji za izbor sekundarne lokacije računalniškega centra slovenske policije

Odločitvena skupina je precej natančno ocenila funkcije koristnosti posameznih kriterijev. Tako je bilo ocenjeno, da prinaša agregatni kriterij »soodvisnost lokacij« okrog 60 odstotkov h končni oceni, preostanek pa pripada agregatnemu kriteriju »značilnosti lokacije«. Znotraj »značilnosti lokacije« sestavlja kriterij »lastnosti« okrog 50 odstotkov, kriterija »varnost« in »stroški« pa vsak po 25 odstotkov. V kriteriju »lastnosti« prispeva kriterij »lastnosti glede na okolje« 60 odstotkov, kriterij »lastnosti lokacije« pa 40 odstotkov h končni oceni. Kriterij »kakovost komunikacijskih povezav« je hkrati opredeljen tudi kot izločilni kriterij, saj je za zagotovitev dovolj zanesljivega delovanja sistema nujno potrebna medsebojna povezava obeh lokacij preko dveh neodvisnih telekomunikacijskih omrežij.

Po metodi večkriterijskega odločanja so bile na podlagi navedenih kriterijev tri lokacije izbrane kot primerne. Za vse tri lokacije sta bili narejeni študija izvedljivosti in podrobna varnostna ocena. V okviru študije izvedljivosti so bile narejene natančnejše projekcije možnosti adaptacije objektov glede na denarne in prostorske možnosti ter možnosti uporabe objektov glede na strateške interese policije. Varnostna ocena, ki je potrebna zaradi narave dela policije, je obsegala analizo kazenske problematike na območju lokacije, študijo zunanje ogroženosti ter opis tehničnega in požarnega varovanja objekta.

Študija izvedljivosti je pozneje pokazala, da na eni od teh treh lokacij adaptacije, ki je bila potrebna, ne bi bilo mogoče izvesti v času, ki je bil na razpolago, zato je bila ta izločena. Varnostna ocena preostalih dveh lokacij se ni bistveno razlikovala, zato je bilo vodstvu policije predlagano, da v skladu s svojimi strateškimi interesi izbere za sekundarni center enega od obeh objektov, ki sta bila v tehničnem in varnostnem pogledu približno enakovredna.

4.5.2 Restavriranje decentraliziranih sistemov

Ukrepi za zagotavljanje delovanja informacijskega sistema so se tradicionalno nanašali predvsem na centralizirane sisteme, vendar tudi v zadnjih letih, ko so se decentralizirani sistemi že dokaj široko uveljavili, ni bistveno drugače. Prvi razlog za to tiči v dejstvu, da so decentralizirani sistemi začeli resneje prodirati v poslovno informatiko šele pred dobrim desetletjem in da se v večini večjih organizacij, kjer se navadno namenja večja pozornost ukrepom za zagotavljanje poslovanja, na takih sistemih še vedno izvaja sorazmerno majhen delež kritičnih aplikacij. Drugi razlog pa je v tem, da se ti sistemi zaradi svoje razpršene in med sabo zelo različne zasnove izmikajo standardnim pogledom glede uvajanja ukrepov za restavriranje delovanja strojne opreme in da se v praksi pojavlja relativno malo uporabnih postopkov, ki bi bili primerni za širši krog tako oblikovanih informacijskih sistemov.

4.5.2.1 Lastnosti decentraliziranih sistemov

Decentralizirani informacijski sistemi vsebujejo v nasprotju s centraliziranimi več fizično ločenih procesnih enot, ki se navadno nahajajo v različnih delih organizacije bližje končnim uporabnikom. Topologija tovrstnih sistemov je lahko zelo različna, saj se aplikacije lahko izvajajo bodisi na strežnikih, ko gre za uporabo tankih odjemalcev, bodisi na odjemalcih, ko gre za uporabo debelih odjemalcev, bodisi na obeh ravneh. Še bolj pisana slika je pri načinu hranjenja in manipuliranja s podatki, saj so ti lahko razpršeni po strežnikih, lahko so centralizirani na enem pomnilniškem sistemu ali pomnilniški mreži, lahko so replicirani na različnih strežnikih, lahko pa se uporablja tudi kombinacija navedenih možnosti.

Na splošno velja, da imajo decentralizirani sistemi prednost pred centraliziranimi zaradi svoje žilavosti. Zaradi fizične razpršenosti strojne opreme je namreč le malo možnosti, da bi bil celotni informacijski sistem hkrati prizadet zaradi istega vzroka. Po drugi strani pa za decentralizirane sisteme vendarle velja, da so bolj ranljivi od centraliziranih gledano s stališča možnosti za delni izpad njihovega delovanja. Nekaj razlogov za to je navedenih v nadaljevanju.

- Za delovanje strojne in sistemske programske opreme centraliziranih sistemov navadno neprestano skrbi skupina visoko specializiranih sistemskih inženirjev, skrbnikov in operaterjev, medtem ko to pri decentraliziranih sistemih ni v navadi.
- Topologija decentraliziranih sistemov je zapletena, poleg tega je strojna oprema pri teh sistemih navadno nehomogena, zato je precej več možnosti, da pride do okvar, pri čemer sta diagnosticiranje in odprava napak težja kakor pri centraliziranih sistemih.
- Strojna oprema decentraliziranih sistemov se pogosto nahaja v manj primernih prostorih in je slabše varovana, zaradi česar je več možnosti, da pride do okvar.
- Sistemska programska oprema, tudi operacijski sistemi, je v decentraliziranih sistemih bistveno manj zanesljiva kakor v centraliziranih. Povprečna razpoložljivost operacijskega sistema Windows, na primer, je približno 99,5-odstotna, kar pomeni na leto okrog 50 ur izpada, medtem ko je povprečna razpoložljivost operacijskega sistema z/OS 99,999-odstotna, kar pomeni na leto približno pet minut nepredvidenega izpada. Podobno ali še slabše razmerje velja tudi za drugo strojno in sistemsko programsko opremo na manjših platformah.

Zaradi svoje povsem drugačne zasnove je pri postopkih za restavriranje decentraliziranih sistemov neuporabna večina metod, ki se sicer s pridom uporablja pri centralno zasnovanih sistemih. Zaradi fizične razpršenosti podatkov jih je izjemno težko kopirati na način, ki bi omogočal sinhronizacijo podatkov ob potrebi po njihovem restavriranju. Poleg tega je zaradi fizične razpršenosti aktivne računalniške opreme celotni informacijski sistem praktično nemogoče »klonirati« na način, kot se to vedno pogosteje dela pri centralnih sistemih s postavitvijo delujočih ali mirujočih sekundarnih centrov. Prav zaradi pomanjkanja ustreznih tehničnih možnosti se uvajanje pogojev za zagotavljanje delovanja pri decentraliziranih sistemih zelo pogosto zanemarja.

V zadnjih letih se je na decentralizirane sisteme preselilo precej kritičnih poslovnih aplikacij, kot so na primer aplikacije za načrtovanje virov podjetja, upravljanje preskrbovalnih verig, upravljanje odnosov s strankami ali pa širok razpon tako imenovanih e-storitev, zato postaja tudi potreba po zagotavljanju delovanja tovrstnih sistemov čedalje večja. Ker klasične metode restavriranja decentralizirane strojne opreme v ta namen niso uporabne, je treba uporabiti katero od alternativnih metod. Metode se med sabo zelo razlikujejo po kompleksnosti, funkcionalnosti in ceni, zato je treba precej pazljivosti pri izbiri.

4.5.2.2 Metode restavriranja decentraliziranih sistemov

Metode, s katerimi je mogoče restavrirati delovanje decentraliziranih sistemov, lahko razdelimo v dve skupini. V prvo sodijo metode, ki izkoriščajo žilavost kot temeljno prednost decentraliziranih sistemov. Zaradi množice fizično razpršenih procesorskih in podatkovnih virov je namreč mogoče zagotoviti delovanje sistema tudi ob izpadu katerega od njegovih elementov.

Druga skupina metod pa stavi na centralizacijo nekaterih virov decentraliziranih sistemov. S centralizacijo namreč postanejo uporabne nekatere preskušene in učinkovite metode restavriranja strojne opreme centraliziranih sistemov. Nekatere najpogosteje uporabljene alternativne metode so navedene v nadaljevanju.

- ***Replikacija podatkov.*** Podatki se redno kopirajo na vse strežnike, tako da se na vsakem strežniku nahaja popolna kopija podatkov, in ne samo del. S to metodo je mogoče kadar koli restavrirati podatke, ki so bili na posamezni lokaciji izgubljeni. Metod za replikacijo je več: mogoče je redno popolno kopiranje, na primer enkrat na dan, mogoče pa je tudi asinhrono kopiranje podatkovnih sprememb z uporabo katerega od sporočilnih (*message queuing*) sistemov.
  Metoda zagotavlja delovanje sistema le za uporabnike, ki niso povezani na strežnik, ki je v izpadu. Ti uporabniki pa ostanejo brez informacijske podpore do ponovne vzpostavitve delovanja izpadlega strežnika.

- ***Redundantni strežniki.*** Navedeno pomanjkljivost gornje metode je mogoče odpraviti s tem, da se ob izpadu posameznega strežnika prenese obremenitev na drug, delujoči strežnik. Metoda ima več možnih različic implementacije. Na lokaciji se lahko nahaja redundantni strežnik, ki prevzame obremenitev ob okvari glavnega strežnika. Ta metoda je relativno enostavna za izvedbo, vendar pa ne rešuje problema nesreče, ki prizadene celotno lokacijo in povzroči hkratni izpad obeh strežnikov.
  Problem izpada celotne lokacije je mogoče rešiti s prenosom obremenitve na drug strežnik, ki se nahaja v istem sistemu, a na drugi lokaciji. Za tak način prenosa za zdaj ni pripravljenih »tovarniških« tehnoloških rešitev, pač pa je za izrabo te možnosti treba ustrezno oblikovati aplikacije in vpeljati prilagojene komunikacijske protokole.
  Tak način prenosa obremenitve je izjemno učinkovit, vendar pa tudi izjemno zapleten za implementacijo in vzdrževanje. Primer komunikacijskega protokola, ki omogoča tako neodvisno delovanje, je TCP/IP oziroma internet.

- ***Redundantna aplikacija na centralnem strežniku.*** Pri tej metodi služi centralni sistem kot nadomestilo v primeru izpada decentraliziranega sistema. Uporaba te metode je smiselna le v primeru, če v organizaciji že obstajata oba sistema in je mogoče centralni sistem začasno uporabiti tudi za izvajanje aplikacij, ki se sicer izvajajo na razpršenih strežnikih. Na centralnem sistemu se lahko izvajajo le

prilagojene aplikacije, tako da je treba pri uporabi te metode vzdrževati dve različni verziji aplikacije.

- ***Združevanje podatkovnih nosilcev.*** Pri tej metodi se podatkovni nosilci razpršenih strežnikov združijo na enem mestu, tako da jih je mogoče kopirati in restavrirati podobno, kot pri centraliziranih sistemih. Če je izvedena centralizacija vseh podatkov in so strežniki brez lastnih diskovnih zmogljivosti, je ob uporabi te metode mogoča tudi hitra in neproblematična menjava okvarjenih strežnikov. Pogoj za uporabo te metode so dobre telekomunikacijske povezave, poleg tega je treba paziti tudi, da strežniki niso preveč oddaljeni od lokacije s podatkovnimi nosilci, da ne bi prišlo do težav z odzivnimi časi.

- ***Konsolidacija strežnikov.*** Poleg podatkovnih nosilcev je mogoče na skupno platformo združiti tudi strežnike, pri čemer pa posamezni strežniki delujejo avtonomno. Tako združene strežnike je mogoče obravnavati kot centralni sistem in jih na tak način tudi restavrirati. Rešitev je relativno nova in vsaj za zdaj uporabna le za nekatere vrste strežnikov, njena implementacija pa prinaša tudi precejšnje spremembe v topologiji informacijskega sistema.

Zadnji navedeni metodi sodita že v področje reinženiringa poslovnih informacijskih sistemov, kjer se v zadnjem času krepi pritisk v smeri ponovne centralizacije ali konsolidacije virov. Razlogov za premik v smeri centralizacije je več, eden od njih pa je prav gotovo tudi enostavnejše zagotavljanje delovanja ob izpadu pri centraliziranih informacijskih sistemih. Obstaja vrsta načinov konsolidacije, ki pa večidel vse temeljijo na močnih telekomunikacijskih povezavah, mrežni tehnologiji in zamenjavi debelih odjemalcev s tankimi.

4.5.2.3 Restavriranje informacijske opreme končnih uporabnikov

V sklop restavriranja razpršene strojne opreme sodi tudi restavriranje informacijske opreme končnih uporabnikov. Ta problem je na prvi pogled manj pomemben, saj izpad informacijske podpore pri posameznem končnem uporabniku za delovanje organizacije nima tako ključnega pomena, da bi se bilo treba posebej zadrževati pri tem. Če pride do okvare posameznega strežnika ali delovne postaje posameznega uporabnika, ki ju je mogoče relativno enostavno in hitro zamenjati, to tudi drži. Teža problema pa se precej spremeni v primeru, kadar zaradi večje nesreče ni več mogoče opravljati dela v celotnem objektu, in je treba obnoviti delovanje na drugi lokaciji.

V tem primeru se problem restavriranja strojne opreme končnega uporabnika pravzaprav preobrazi v problem ponovnega vzpostavljanja ustreznega delovnega okolja. Poglavitna dela, ki jih je pri tem treba opraviti, so naslednja:

- poiskati in po potrebi opremiti primerne nadomestne prostore,
- preusmeriti telekomunikacijske podatkovne in zvočne ter poštne povezave na novo lokacijo,
- obnoviti informacijsko opremo in vzpostaviti možnosti za njeno delovanje,
- obvestiti zaposlene in po potrebi pripraviti poskrbeti za prevoz/namestitev na nadomesti lokaciji.

4.5.2.4 Metode zagotavljanja delovanja na ravni končnega uporabnika

Način izvajanja naštetih dejavnosti sodi v okvir okrevalnega načrta organizacije. Ker je razkorak med potrebnimi sredstvi za zagotavljanje delovanja in potencialno škodo, ki jo lahko povzroči izpad, na tej ravni največji, se prav tu kažejo med organizacijami največje razlike pri načrtovanju ukrepov. Načinov reševanja problema obnavljanja delovanja na ravni končnega uporabnika je veliko in se med organizacijami lahko zelo razlikujejo, zato so v nadaljevanju navedeni samo nekateri najbolj značilni (Toigo, 2000, str. 222–227).

- ***Brez vnaprejšnje priprave.*** Tak način pomeni, da je treba vse prej navedene dejavnosti za vzpostavitev nadomestnih prostorov opraviti po uničenju poslovnih prostorov organizacije. Ta način je seveda najcenejši, poleg cenovnega pa je poglavitni razlog, da se odločimo zanj, tudi v splošnem prepričanju, da naj bi v mestnih območjih vendarle obstajale dovolj velike prostorske in telekomunikacijske zmogljivosti, ki jih je mogoče v kratkem času pridobiti in prilagoditi. Kljub temu ima ta način veliko pomanjkljivosti, saj se vse dejavnosti, od katerih lahko nekatere vendarle terjajo kar precej časa, izvajajo v času, ko je delovanje že ustavljeno, kar lahko pomembno podaljša čas do ponovne vzpostavitve delovanja. Poleg tega obstaja nevarnost, da zaradi nesreče večjega obsega vendarle ne bo na razpolago dovolj nadomestnih zmogljivosti.

- ***Vnaprej vzpostavljene nadomestne zmogljivosti.*** To je najdražja rešitev, katere uporaba je smotrna le v primeru, kadar organizacija razpolaga z več med sabo primerno oddaljenimi objekti, v katerih je na razpolago dovolj rezervnega prostora. V takem primeru je mogoče določiti razpoložljivi prostor v teh objektih za nadomestne zmogljivosti in jih vnaprej primerno opremiti. Prednost te rešitve je predvsem v tem, da je brez težav mogoče celotni postopek selitve delovanja načrtovati vnaprej, zaradi česar ga je mogoče izvesti v zelo kratkem času in z najmanj težavami. Slabost je predvsem visoka cena.

- ***Kombinirana rešitev.*** Organizacija se lahko odloči tudi za kombinirano rešitev, ki združuje oba navedena načina. Pri nesrečah lokalnega obsega se uporabi način brez vnaprejšnje priprave, saj je v takih primerih vendarle več verjetnosti, da bo mogoče dobiti primerne nadomestne zmogljivosti v bližini in jih v relativno kratkem času usposobiti. Za primer regionalne nesreče pa ima organizacija pripravljen načrt selitve poslovanja na dovolj oddaljeno nadomestno lokacijo. Tovrstna kombinacija obeh prejšnjih načinov seveda združuje tudi njune prednosti in slabosti.

- ***Delo na daljavo.*** Možnost dela na daljavo ali dela na domu je v informatiki v uporabi že kar nekaj časa, vendar je dobila veljavo šele v zadnjih letih, in sicer z izrazitim povečanjem javnih telekomunikacijskih zmogljivosti in s pojavom interneta. To možnost je, resda v omejenem obsegu, mogoče s pridom izkoristiti tudi za vzpostavitev delovanja v primeru uničenja poslovnih prostorov. Pri tem je treba zagotoviti delovanje mrežne komunikacijske strojne opreme, poleg tega je pogoj tudi delovanje javnega telekomunikacijskega omrežja. Gre za relativno novo in za zdaj še precej nepreizkušeno rešitev, ki je zelo učinkovita, hkrati pa tudi relativno poceni, tako da utegne v prihodnosti igrati zelo pomembno vlogo pri reševanju problema ponovne vzpostavitve delovnega okolja končnih uporabnikov.

4.5.3 Največji obseg restavriranja strojne opreme

Ko rešujemo problem, kako ponovno vzpostaviti delovanje na ravni končnih uporabnikov, se je treba pomuditi tudi pri premisleku, ki se pravzaprav nanaša na celotno problematiko uvajanja pogojev za ponovno vzpostavitev delovanja informacijskega sistema. Vprašanje, ki se pri tem pojavlja, je, kolikšen obseg si organizacija pri tem še lahko privošči oziroma na kakšen obseg izpada se je še smotrno pripravljati.

Obstaja namreč neka zgornja meja posledic nesreče, do katere je še smotrno načrtovati obnavljanje poslovanja v stari obliki oziroma v starem okviru. Ob nesreči, katere posledice presegajo tak obseg, pa nima smisla tratiti sredstev in truda za ponovno vzpostavljanje poslovanja, pač pa je bolj smotrno poslovanje prenehati. Nadaljnji postopki v takih primerih so zelo različni, odvisni so od obsega in vrste organizacije, od vrste poslovanja, vrste nesreče ipd., njihova obravnava pa presega zasnovo tega dela. V vsakem primeru pa je pri teh postopkih mogoče s pridom izkoristiti podatke, ki so bili kopirani in varovani v okviru postopkov za zagotavljanje delovanja informacijskega sistema organizacije, poleg tega pa v takih primerih ti podatki pomenijo tudi pomemben arhivski vir.

Največji obseg nesreče, do katerega je še smotrno načrtovati ponovno vzpostavljanje delovanja, je težko natančno opredeliti in se od organizacije do organizacije močno razlikuje. Odvisen je od velikosti same organizacije, vrste njenega delovnega področja, obsega in načina delovanja, topologije objektov, ki so v lasti organizacije, ipd. Z natančnimi opredelitvami tega

obsega se organizacije navadno ne ukvarjajo, pač pa so bolj predmet intuitivnega premisleka. V vsakem primeru pa se je pri uvajanju pogojev za zagotavljanje delovanja informacijskega sistema in poslovanja treba zavedati, da je to vendarle namenjeno le premostitvi nesreč z omejenimi posledicami.

4.6 Restavriranje telekomunikacijskih povezav

Telekomunikacijske povezave so eden glavnih pogojev za sodobno poslovanje, še posebno pa za delovanje poslovnih informacijskih sistemov. Pri tem ni pomembna samo povezava med vse večjim številom uporabnikov in strežnikov znotraj organizacije same, pač pa postaja za sodobno poslovanje vse bolj pomembna tudi povezava med organizacijo in njenim okoljem.

Telekomunikacijske povezave so z vidika zagotavljanja poslovanja precej problematične. Eden od razlogov je v tem, da postajajo telekomunikacijske povezave zaradi hitrega razvoja v zadnjih letih in zaradi prepletanja različnih protokolov vse bolj zapletene, zaradi česar se pojavlja vedno več napak v delovanju, diagnosticiranje napak pa postaja vse težavnejše. Drug razlog je v tem, da so telekomunikacijske povezave fizično široko razprostranjene, zaradi česar je možnost okvar precejšnja, poleg tega jih je tudi zelo težko nadzirati. Tretji razlog je v tem, da so povezave do oddaljenih uporabnikov v večini primerov v lasti zunanjih ponudnikov, zaradi česar organizacija na njihovo kakovost in vzdrževanje največkrat nima nobenega vpliva.

Za delovanje sodobnega informacijskega sistema, pa tudi nasploh za poslovanje organizacije, so telekomunikacijske povezave ključnega pomena. Pod tem pojmom se skriva cela vrsta različnih komponent in tehnologij, ki sodijo na področja telekomunikacij v ožjem smislu, informatike in elektronike. Postopki ponovne vzpostavitve različnih komponent omrežnega sistema se med sabo močno razlikujejo, a jih je za obravnavo temeljnih strategij obnove mogoče na grobo razdeliti v tri skupine.

4.6.1 Restavriranje notranjega telekomunikacijskega omrežja

V prvo skupino sodijo tisti elementi telekomunikacijskega sistema, ki se nahajajo znotraj posamezne lokacije in so potrebni za notranje povezave med uporabniki, med sistemi ter med uporabniki in sistemi. V to skupino sodijo na primer lokalna računalniška omrežja, notranja telefonska vozlišča, lokalne povezave pomnilniških sistemov (SAN, NAS), stikala, lokalna ožičenja ipd. Ta del omrežja je navadno v lasti organizacije, v njem pa se tesno prepletajo informacijske in telekomunikacijske prvine. Predvsem v delu, kjer gre za izmenjavo podatkov ali kombinirano podatkovno-zvokovno izmenjavo, je notranji del omrežja dokaj kompleksno okolje, ki je nagnjeno k pogostim okvaram in izpadom.

Uvajanje metod nadzora nad lokalnimi sistemi, predvsem to velja za podatkovne dele omrežja, ter uvajanje redundantnih aktivnih elementov omrežja sta edini metodi, ki ju je za zagotavljanje delovanja v tem delu mogoče uporabiti. Zaradi relativne prostorske omejenosti tega dela omrežja in relativno nizke cene posameznih komponent uvajanje redundantnih zmogljivosti finančno navadno ni problematično, treba je le jasno opredeliti postopke prenosa obremenitve.

Vendar pa je treba upoštevati, da pri pojavljanju nestabilnosti v lokalnih podatkovnih omrežjih, ki nastajajo zaradi neusklajene mrežne strojne opreme, uporabe različnih komunikacijskih protokolov, neustrezne konfiguracije omrežja ipd., uvedba redundantnih zmogljivosti ne pomaga. V takih primerih je edina rešitev prenova omrežja, ki pa je v finančnem, predvsem pa v tehnološkem pogledu zelo zahteven poseg.

4.6.2 Restavriranje povezovalnih komponent

V drugo skupino omrežnega sistema sodijo komponente, katerih naloga je povezati notranje uporabnike in sisteme s prostranim zunanjim omrežjem. Sem sodijo, denimo, usmerjevalniki, modemi, požarni zidovi, naprave DWDM, ISDN ali SDH adapterji, povezave do vozlišč telekomunikacijskih ponudnikov ipd. Komponente tega omrežnega segmenta sodijo dokaj izrazito na telekomunikacijsko področje, zato večina organizacij njihovo vzdrževanje raje prepušča zunanjim izvajalcem.

Edina metoda zagotavljanja delovanja v tem segmentu je uvajanje redundance. To pa je lahko finančno nekoliko bolj problematično, saj so nekatere povezovalne komponente lahko zelo drage. Redundantne komponente morajo biti konfigurirane in dimenzionirane tako, da se lahko obremenitev prenaša samodejno in za uporabnika neopazno.

Poseben problem so tudi fizične povezane na zunanje omrežje oziroma na najbližje vozlišče zunanjega telekomunikacijskega ponudnika. Te povezave so lahko bodisi v lasti organizacije bodisi v lasti zunanjega ponudnika. V vsakem primeru je za zagotavljanje poslovanja treba poskrbeti, da so te povezave izvedene redundantno, kar pa ni vedno enostavno, saj gre za fizično izvedene povezave.

Zunanji ponudnik namreč pogosto lahko zagotavlja redundantno varianto povezave (na primer najeti vod – ISDN), pri čemer pa od najbližjega vozlišča do organizacije obe, sicer logično različni povezavi, tečeta po istem fizičnem vodniku. Primeri takšne navidezne redundance so dokaj pogosti, na primer tudi v slovenski policiji, in terjajo dodatno pozornost (Girard, 2002). Najboljši način reševanja tega problema je, da se vzpostavita dve fizično ločeni povezavi do dveh različnih telekomunikacijskih ponudnikov.

4.6.3 Restavriranje povezav v prostranem omrežju

V tretjo skupino sodijo vse telekomunikacijske komponente, ki se nahajajo zunaj meja organizacije. V to skupino sodijo javna ali zasebna prostrana omrežja, zunanja telekomunikacijska vozlišča, internet in drugi komunikacijski protokoli ipd. Zunanje telekomunikacijske povezave, razen izjemoma, niso v lasti poslovnega sistema, zato je zagotavljanje nadomestnih povezav ob izpadu primarnih povezav ali ob selitvi računalniškega centra na sekundarno lokacijo v rokah zunanjih telekomunikacijskih ponudnikov, s katerimi organizacija sodeluje. Izjema pri tem so le nekatere državne institucije, ki imajo razvito svoje telekomunikacijsko omrežje, ali pa organizacije, ki se same ukvarjajo s ponudbo telekomunikacijskih storitev.

Zagotavljanje redundantnih povezav v prostranem omrežju je zato problematično iz dveh razlogov. Rešitev s stalnim najemom nadomestnih povezav je zaradi visokih cen najema prenosnih zmogljivosti dokaj draga. Po nekaterih ocenah naj bi na primer stroški za zagotavljanje redundantnih telekomunikacijskih povezav znašali kar okrog tretjino stroškov vzdrževanja dveh oddaljenih računalniških centrov, ki se medsebojno podpirata.

Drug problem pa je zagotavljanje resnične redundance v zunanjem omrežju. Tudi če povezave zagotavljata dva različna telekomunikacijska ponudnika, organizacija nima nikakršnega jamstva, da ponudnika nimata posameznih delov omrežja skupnih. Edina res zanesljiva rešitev je tako zgraditev lastnega omrežja, česar pa si večina organizacij, razen prej omenjenih izjem, ne more privoščiti.

V Sloveniji je problem še bolj pereč, saj premoremo le enega ponudnika telekomunikacijskih povezav, ki je sposoben povezati lokacije po vsej Sloveniji, to je Telekom Slovenije, ki pa sam nima dvojnega hrbteničnega omrežja. Zato je resnično redundanco v prostranem omrežju mogoče doseči le z najemom nadomestnih zmogljivosti pri alternativnih ponudnikih. Ti ponudniki, Elektro-Slovenija, Slovenske Železnice/Telemach in DARS, imajo zgrajena svoja hrbtenična optična omrežja, kjer je mogoče najeti prenosne zmogljivosti. Vendar pa ta omrežja povezujejo le omejeno število krajev po Sloveniji, zaradi česar je možnost njihovega angažiranja dokaj omejena.

Odlična alternativa optičnim telekomunikacijskim povezavam so digitalne radijske povezave. Gre za relativno novo in izjemno žilavo tehnološko rešitev dovolj velike zmogljivosti, da jo je mogoče uporabiti tako za govorne kot za podatkovne komunikacije. Vpeljava digitalnega radia je izjemno draga, zato si jo praktično lahko privoščijo le državne institucije, ki poleg zanesljivosti potrebujejo tudi dostop do področij, kamor zemeljske komunikacije ne sežejo.

Slovenska policija je leta 2003 začela postavljati prve postaje digitalnega radijskega omrežja, ki se bo predvidoma v petih letih razširilo čez celotno slovensko ozemlje in naj bi ga uporabljale vse zainteresirane državne institucije. Predvideno je, da bi se digitalni radio

uporabil tudi kot nadomestna telekomunikacijska povezava za prenos podatkov med uporabniki in računalniškim centrom slovenske policije v Ljubljani.

4.7 Vzpostavitev poslovanja

Poleg tehničnih detajlov je treba pri izdelavi okrevalnega načrta precejšnjo pozornost nameniti tudi organizacijskemu delu. Še tako natančno izdelani, dragi in dosledno implementirani tehnični ukrepi za zagotavljanje delovanja informacijskega sistema ne zaležejo kaj dosti, če niso primerno organizacijsko podprti. Da je načrt zasnovan organizacijsko neustrezno, se največkrat pokaže šele, ko nastane resnična potreba po uveljavitvi ukrepov – na primer zaradi nesreče – in ko je že prepozno, da bi ga kakor koli spreminjali.

Osrednja vloga pri vzpostavljanju delovanja informacijskega sistema in zagotavljanju poslovanja organizacije pripada, ne glede na izbrano tehnično rešitev, ljudem. Zelo zgoščeno je organizacijska stran okrevalnega načrta opisana v literaturi kot »kdo in v kakšnem primeru sproži njegovo izvajanje ter kdo pri tem dela kaj in kdaj« (Toigo, 2000, str. 287).

4.7.1 Ravnanje ob izrednem dogodku

Ne glede na to, ali pride do načrtovanega ali nenačrtovanega izpada informacijskega sistema, je treba v obeh primerih izvesti enake postopke za ponovno vzpostavitev delovanja. Vendar pa je razlika med primeroma v tem, da sta čas in obseg izpada pri načrtovanem izpadu izbrana, zato je vse postopke mogoče načrtovati in jih delno tudi izpeljati vnaprej, poleg tega so v tem primeru na razpolago vsi viri, ki so za vzpostavitev delovanja potrebni. Nič od tega pa navadno ne drži v drugem primeru, ko je dogajanje največkrat povsem nepredvidljivo. Zato je v organizacijskem delu okrevalnega načrta treba nameniti posebno pozornost prav vzpostavitvi poslovanja ob nepredvidenem izpadu, medtem ko prenos delovanja ob načrtovanih izpadih navadno sodi v opis rednih delovnih postopkov.

Gartner svetuje, da mora organizacija ob izpadu informacijskega sistema zaradi večje nesreče ali okvare ravnati po načelih kriznega menedžmenta. Le ustrezno in učinkovito ravnanje v takih primerih lahko prepriča zaposlene, stranke, partnerje, investitorje in zunanjo javnost, da je organizacija sposobna premagati težave in si tako zagotoviti njihovo zaupanje. V okrevalnem načrtu morajo biti za vzpostavljanje poslovanja opredeljeni naslednji organizacijski elementi (Younker, 2001):

- okrevalne ekipe in naloge, ki jih morajo izvesti,
- postopki obveščanja in transporta ljudi ter opreme,
- diagram dejavnosti – povezave med nalogami.

4.7.2 Oblikovanje okrevalnih ekip

Prva in najpomembnejša organizacijska naloga okrevalnega načrta je oblikovanje ekip in opredelitev njihovih nalog. Na vrsto in sestavo okrevalnih ekip sicer pomembno vpliva izbira tehnološke rešitve ukrepov za zagotavljanje delovanja informacijskega sistema, vendar pa je pri tem mogoče upoštevati tudi nekatera splošna priporočila. Toigo tako navaja naslednje okrevalne ekipe in njihove naloge, pri čemer poudarja, da sta velikost in zasedenost ekip močno odvisni od velikosti organizacije, da je nekatere ekipe mogoče združiti, nekatere pa po potrebi razdeliti v podskupine (Toigo, 2000, str. 298–301).

- ***Koordinacijska ekipa.*** Koordinira dejavnosti.
- ***Ekipa na sekundarni lokaciji.*** Skrbi za pomnilniške medije na oddaljeni lokaciji in njihov transport ob potrebi po restavriranju.
- ***Ekipa sistemskih inženirjev.*** Odgovorna za vzpostavitev strežniške sistemske programske opreme.
- ***Ekipa aplikacijskih programerjev.*** Odgovorna za vzpostavitev delovanja uporabniške programske opreme, tako na strežniški strani kot pri končnih uporabnikih.
- ***Ekipa za prostrane omrežne povezave.*** Sodeluje s ponudniki telekomunikacijskih storitev pri vzpostavljanju nadomestnih prostranih omrežnih povezav.
- ***Ekipa za lokalne omrežne povezave.***
- ***Ekipa za strojno opremo.*** Odgovorna za namestitev uporabniške strojne opreme.
- ***Ekipa za transport.*** Odgovorna za transport ljudi in opreme na oddaljeno lokacijo, lahko je odgovorna tudi za vzpostavitev take lokacije, če ta ni že vnaprej določena.

Fulmer priporoča precej enostavnejšo strukturo, pri čemer poudarja, da se je pri sestavi okrevalnih ekip treba ozirati na posebne zahteve, ki jih terjajo razmere ob ponovnem vzpostavljanju delovanja informacijskega sistema. Zato je organizacijska struktura okrevalnih ekip drugačna od siceršnje strukture v organizaciji, ekipe pa so lahko po potrebi dopolnjene tudi s člani, ki sicer niso zaposleni v organizaciji (Fulmer, 2000, str. 64–66):

- ***Ekipa za izredne razmere.*** Odgovorna za koordiniranje dejavnosti, uresničevanje okrevalnega načrta, obveščanje in komuniciranje.
- ***Ekipa za rekonstrukcijo.*** Odgovorna za rekonstrukcijo primarne lokacije; v okvir njenega delovanja sodi vse od ocene škode do koordiniranja dejavnosti za ponovno vzpostavitev delovanja na primarni lokaciji.
- ***1. ekipa na oddaljeni lokaciji.*** Odgovorna za vzpostavitev ali zagon sekundarne lokacije, postavitev strojne opreme, vzpostavitev telekomunikacijskih povezav ter prevoz opreme in ljudi na oddaljeno lokacijo.
- ***2. ekipa na oddaljeni lokaciji.*** Odgovorna za postavitev sistemske in uporabniške programske opreme na sekundarni lokaciji ter vzpostavitev delovanja.

Pri sestavi ekip je poleg značilnosti informacijskega sistema, izbrane okrevalne rešitve in morebitnih posebnih zahtev organizacije treba upoštevati tudi dejstvo, da v kritičnem trenutku vsi potrebni ljudje ne bodo na razpolago. Povsem mogoče je namreč, da bodo nekateri člani poškodovani ali nedosegljivi, da ne bodo mogli pravočasno priti na dogovorjeno lokacijo ipd.

Na problem dosegljivosti članov okrevalnih skupin je treba računati že pri izdelavi okrevalnega načrta, pri čemer je treba iskati rešitve v dveh smereh. Prvič morajo biti ekipe, če je to le mogoče, sestavljene redundantno, z večjim številom članov ali z nadomestnimi člani. Če v organizaciji ni na voljo dovolj ustreznih ljudi, je dobro iskati pomoč pri zunanjih izvajalcih, seveda pod pogojem, da so ti tako pomoč sposobni tudi dejansko zagotoviti.

Druga pomembna ugotovitev, ki izhaja iz problema dosegljivosti ljudi in jo je treba pri izdelavi okrevalnega načrta nedvomno upoštevati, pa je ta, da mora biti načrt kar se da enostaven za izvedbo in čim bolj avtomatiziran. Tako je mogoče doseči, da bodo dejavnosti, predvidene z načrtom, izpeljane tudi tedaj, ko kdo od ključnih članov ekip ne bo mogel sodelovati pri njihovi izvedbi.

4.7.3 Medsebojno obveščanje ob izrednih dogodkih

Naslednji pomemben organizacijski element, ki ga mora vsebovati okrevalni načrt, je način obveščanja. V načrtu morajo biti natančno opredeljeni postopki obveščanja, kjer je treba določiti, kdo obvešča koga in kdaj ter kako bo medsebojno obveščanje potekalo. Medsebojnemu obveščanju je treba nameniti posebno pozornost predvsem zato, ker je mogoče utemeljeno pričakovati, da bodo ob večji nesreči možnosti obveščanja občutno omejene. Prav zato morajo biti postopki medsebojnega obveščanja zasnovani dovolj žilavo oziroma robustno, da bodo delovali tudi v težko predvidljivih razmerah, nastalih ob večjih nesrečah.

Najpogosteje se za obveščanje ob izrednih situacijah priporoča uporaba tako imenovanega drevesa obveščanja (*Call Tree, Notification Tree*). Tako je mogoče doseči, da odgovornost za obveščanje ni osredotočena v eni točki, pač pa se prenaša niže po »drevesu«, kjer je vsaka točka odgovorna za obveščanje svojih neposredno podrejenih točk. V obveščevalnem drevesu je sorazmerno preprosto opredeliti tudi ustrezno časovno zaporedje in zakasnitve pri prenašanju obvestil na nižje ravni. Vsekakor morajo osebe, ki so odgovorne za obveščanje svojega dela »drevesa«, vnaprej natančno vedeti, koga obvestiti in kako, kar mora biti jasno opredeljeno v okrevalnem načrtu.

Pomembna je tudi redundanca komunikacijskih poti. Povsem mogoče je namreč, da bodo ob večji regionalni nesreče, na primer ob potresu, zemeljske telefonske povezave prekinjene. Zato je treba za obveščanje predvideti tudi alternativne komunikacijske možnosti, kot so na

primer mobilni telefoni, druge brezžične komunikacijske naprave, internetne povezave ipd.. Med napadom na Svetovni trgovinski center v New Yorku 11. septembra 2001 se je na primer pokazalo, da so bile alternativne povezave z uporabo internetne elektronske pošte, elektronskega klicanja ipd. za medsebojno obveščanje zelo učinkovite (Wheatman, 2001).

4.7.4 Dejavnosti okrevalnega načrta

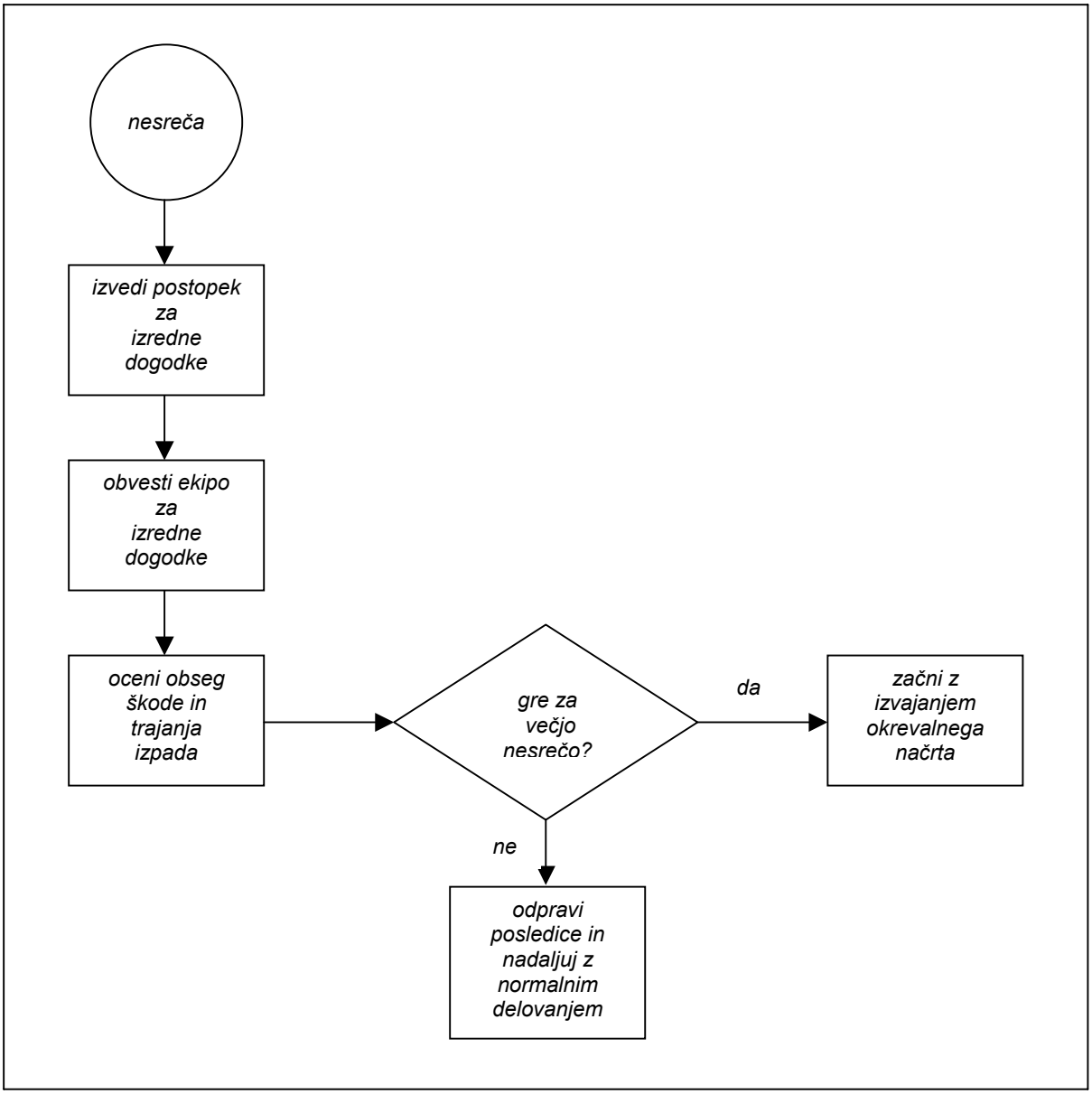
Osrednji del okrevalnega načrta sestavljajo opisi dejavnosti, ki jih morajo ekipe in posamezniki izvesti ob prekinitvi delovanja informacijskega sistema. Načrt mora biti kar najbolj pregleden in preprost, tako da ga je mogoče izpeljati tudi, če dokumentacija ni na razpolago. Tudi naloge, predvidene v okrevalnem načrtu, morajo biti dovolj enostavne, da jih je mogoče izvesti tudi tedaj, ko ni vseh ključnih ljudi na razpolago. Člani okrevalnih ekip morajo imeti pri sebi opomnike glede svojih nalog v okviru okrevalnega načrta, temeljne postopke pa morajo poznati na pamet.

Dejavnosti okrevalnega načrta je mogoče prikazati na različne načine, med drugim tudi z diagrami dejavnosti, s katerimi je mogoče preprosto in pregledno prikazati medsebojne odnose med dejavnostmi. Primer preprostega diagrama dejavnosti za postopek odločitve o začetku izvajanja okrevalnega načrta je prikazan na sliki 11 (Toigo, 2000, str. 311).

4.7.5 Odločitev za začetek uresničevanja okrevalnih dejavnosti

Primer diagrama dejavnosti za odločitev o uresničitvi okrevalnega načrta je izbran zato, ker mora biti ta del dejavnosti z manjšimi razlikami sestavni del vsakega načrta, ne glede na njegove siceršnje tehnološke značilnosti. Dejstvo je, da je ne glede na stopnjo avtomatizma pri uresničevanju načrta, v tem delu okrevalnega postopka potrebna eksplicitna odločitev: oseba ali skupina, ki ji je podeljena ta odgovornost, mora na podlagi ocene nepričakovanega kriznega dogodka odločiti, ali gre za večjo nesrečo oziroma katastrofo in je treba začeti postopke prenosa delovanja ali ne. Razlog za to je dejstvo, da do prekinitve delovanja lahko pride iz preveč različnih možnih razlogov, da bi bilo mogoče oceno o kritičnosti dogodka prepustiti avtomatizmu. Tudi pri povezavi dveh računalniških sistemov GDPS, kjer je postopek prenosa delovanja sicer popolnoma avtomatiziran, tega postopka v nobenem primeru ne more pognati sistem sam.

Odločitev za začetek prenosa delovanja informacijskega sistema temelji na ocenah obsega in trajanja izpada, ki skupaj tvorita oceno posledic izpada za poslovanje organizacije. Elementi za sprejem odločitve za izvedbo prenosa na podlagi omenjenih ocen morajo biti opredeljeni v okrevalnem načrtu. Seveda pa v okrevalnem načrtu ni mogoče predvideti vseh možnosti, zato v vsakem primeru ostaja precej odgovornosti za sprejem odločitve na ramenih tistega, ki mora ob kriznem dogodku odločitev sprejeti.



Slika 11: Primer diagrama dejavnosti za odločitev o izvajanju okrevalnega načrta (Vir: Toigo, 2000, str. 311)

Najprej je treba ugotoviti vzrok oziroma vrsto okvare, kar morajo narediti strokovnjaki iz organizacije ali izven nje, ki upravljajo informacijski sistem. Treba je ugotoviti, kateri del informacijskega sistema je zaradi nepredvidenega dogodka v okvari, in presoditi, ali je posledice mogoče odpraviti ter nadaljevati delovanje na osnovnem sistemu in v kolikšnem času je to mogoče narediti. Poleg vzroka je treba oceniti tudi obseg izpada oziroma delež uporabnikov, ki zaradi izpada ostaja brez informacijske podpore.

Vzrok in obseg izpada je navadno mogoče ugotoviti relativno hitro, precej težje pa je natančneje oceniti predvideno trajanje izpada. Pri velikih nesrečah, kot so na primer poplave,

večji požari ali potresi, ta ocena niti ni tako pomembna, saj so zaradi obsega dogodka v vsakem primeru podani vsi pogoji, da se preide z delovanjem na alternativni sistem. Vendar pa so takšni primeri dokaj redki, saj povzročijo le od tri do pet odstotkov vseh izpadov informacijske podpore. Veliko večino izpadov pa povzročijo tehnične okvare na strojni opremi, prekinitve telekomunikacijskih povezav, programske napake, napake zaposlenih, vdori ipd. Za tovrstne izpade je v večini primerov težko predvideti trajanje, še posebno zato, ker je za oceno na voljo zelo malo časa.

Odločitev za prenos delovanja na alternativni informacijski sistem nikakor ni enostavna. Prenos delovanja ne glede na izbrano tehnično rešitev zahteva precej truda, sredstev, sprememb v organizaciji dela ipd. Pri tem je v večini primerov treba upoštevati tudi to, da bo pozneje treba izpeljati še prenos nazaj na primarni sistem, na kar se pogosto pozablja. Zato mora biti odločitev dobro utemeljena in pretehtana, da ne bi bila s prenosom povzročena večja škoda, kakor bi jo povzročil sam izpad informacijske podpore. Odločitev zato ne bi smela biti sprejeta, dokler ni ugotovljena dovolj velika verjetnost, da bosta trajanje in obseg izpada imela tako velike posledice za poslovanje organizacije, da je uporaba alternativnih rešitev upravičena. Po drugi strani pa je odločitev treba sprejeti čim hitreje, saj čas sprejemanja odločitve podaljšuje čas ponovne vzpostavitve delovanja informacijskega sistema.

4.7.6 Vodenje okrevalnih dejavnosti

Pri izdelavi organizacijskega dela okrevalnega načrta je treba določiti tudi lokacijo, od koder se bodo dejavnosti prenosa informacijske podpore izvajale oziroma koordinirale. Za ta namen je najbolje izbrati sekundarno lokacijo, če je ta izbrana že vnaprej, saj je najprimerneje, da se strokovnjaki nahajajo čim bliže delujočega računalniškega centra. Poleg tega mora biti sekundarna lokacija primerno telekomunikacijsko opremljena, tako da je od tam najlaže vzpostaviti stik z vsemi perifernimi deli organizacije in z okoljem. Pri izbiri alternativnih rešitev brez obstoječe nadomestne lokacije pa je treba vnaprej izbrati oddaljeno »štabno« lokacijo in jo primerno telekomunikacijsko opremiti.

Vendar pa se v praksi na to pogosto pozablja. Zaradi zmanjševanja stroškov se namreč tudi pri vnaprej izbranih in opremljenih sekundarnih lokacijah mnogokrat zagotavljajo le tehnični pogoji delovanja nadomestnega informacijsko-telekomunikacijskega centra. V primerih, ko primarna lokacija ni tako prizadeta, da ne bi bilo mogoče od tam voditi postopka prenosa delovanja, to niti ni tako pomembno, vendar pa je treba v okrevalnem načrtu predvideti tudi možnost, da to ne bo mogoče. Predvidena postavitev povezave dveh računalniških sistemov v slovenski policiji bo omogočala vodenje celotnega postopka prenosa in upravljanje nadomestnega sistema tako s primarne kot sekundarne lokacije. Na sekundarni lokaciji bo stalno na voljo posebna »operatorska soba«, poleg tega je predvidenih še nekaj dodatnih prostorov, ki bodo primerno komunikacijsko opremljeni in jih bo po potrebi v najkrajšem času mogoče pripraviti za uporabo v ta namen.

Pri izdelavi okrevalnega načrta je treba imeti pred očmi dejstvo, da dogodki v nepredvidenih in kriznih situacijah ne potekajo po predvidenih načrtih, ne glede na to, kako skrbno so ti pripravljeni. Upoštevati je treba tudi, da strokovnjaki v organizacijah z izrednimi razmerami nimajo izkušenj, zato je ne glede na pogostnost in resnost testiranja, dejansko ravnanje ljudi v izrednih razmerah težko predvideti. Poleg tega je treba računati tudi z dokaj realno možnostjo, da v izrednih razmerah marsikateri, tudi ključni ljudje iz tega ali onega razloga ne bodo mogli sodelovati pri izvedbi načrta. Zaradi vsega tega mora biti okrevalni načrt v tehničnem in organizacijskem smislu načrtovan čim bolj preprosto, tako da ga je mogoče po potrebi med samim izvajanjem spreminjati in prilagajati ter da ga je mogoče izvesti tudi s pomanjkljivimi in strokovno nepopolnimi ekipami.

5 Testiranje in vzdrževanje načrta

Okrevalni načrt je osrednja točka vsakršne strategije za zagotavljanje delovanja informacijskega sistema in izraža pripravljenost organizacije za reševanje problema izpada informacijske podpore ter njeno pripravljenost na posledice, ki jih tak izpad pomeni za njeno poslovanje. Dobro izdelan načrt pomeni vrh prizadevanja vrste strokovnjakov z različnih področij in naj bi organizaciji zagotavljal jamstvo za preživetje kriznih situacij. Ne glede na ves vloženi trud pri oblikovanju načrta in implementaciji tehničnih rešitev, ki jih načrt predvideva, pa delo na okrevalnem načrtu z njegovo formalno izdelavo nikakor ni končano.

5.1 Usposabljanje članov okrevalnih ekip

Po končani izdelavi okrevalnega načrta je najprej treba usposobiti vse tiste, ki bodo sodelovali pri izvajanju predvidenih postopkov. To velja ne glede na to, ali so načrt sestavili v sami organizaciji ali pa so ga naredili zunanji strokovnjaki. V zadnjem primeru sta predaja znanja in skrbništva nad načrtom tako ali tako sestavni del same izdelave načrta, vendar pa je usposabljanje potrebno tudi v primeru, da je bil načrt izdelan z lastnim znanjem. Pri implementaciji okrevalnih postopkov bodo namreč zagotovo sodelovali tudi ljudje, ki pri izdelavi načrta sicer niso sodelovali ali pa je bilo njihovo sodelovanje minimalno.

Namen usposabljanja je predvsem seznaniti vse tiste, ki bodo sodelovali pri vzpostavljanju nadomestnih informacijskih in telekomunikacijskih rešitev, z njihovimi vlogami pri teh postopkih. Usposabljanje naj bi potekalo ločeno za posamezne okrevalne ekipe in naj bi bilo usmerjeno predvsem na posamezne dejavnosti, ki morajo biti opravljene v okviru nalog

posamezne ekipe, poleg tega pa mora biti vsaj v grobih obrisih prikazan tudi grobi obris vseh dejavnosti v okviru načrta. Vodjem posameznih ekip mora biti predstavljena predvsem splošna slika dogajanja in naloge pri koordinaciji dejavnosti med ekipami.

Predavanja morajo biti dobro pripravljena in dokumentirana, saj jih bo treba pozneje še večkrat ponavljati za sodelavce, ki se bodo ekipam pridružili pozneje, bodisi zaradi zamenjave osebja bodisi zaradi razširitve nalog. Za posamezne naloge je treba usposobiti tudi nadomestne člane ekip, ki lahko priskočijo na pomoč ob morebitni odsotnosti svojih sodelavcev.

5.2 Vzdrževanje okrevalnega načrta

Poslovno okolje organizacije se nenehno razvija in spreminja, čemur se posledično prilagaja tudi informacijski sistem organizacije. Ta se poleg tega neprestano spreminja tudi zaradi stalnega in hitrega tehnološkega razvoja informatike in telekomunikacij. Vsem tem spremembam se mora prilagajati tudi okrevalni načrt, sicer lahko kmalu postane le še mrtva črka na papirju, ki organizaciji ne more več zagotavljati potrebne podpore v kriznih trenutkih. Načrt je zato treba stalno vzdrževati in prilagajati, na kar pa se vse prepogosto pozablja.

5.2.1 Spremljanje sprememb

Načinov ugotavljanja potrebe po spremembah v okrevalnem načrtu je več. Prvi in najprimernejši način je s postopkom spremljanja sprememb v informacijskem sistemu (*change menedžment*). Potrebe po popravkih načrta se lahko pokažejo tudi pri testiranju, kjer pridejo na dan pomanjkljivosti, ki nastanejo kot posledica sprememb v sistemu. Tretji način, ki je manj primeren in vsem organizacijam niti ni na voljo, pa so zahteve po spremembah, ki jih zaradi opaženih pomanjkljivosti zahtevajo nadzorne institucije po opravljenem pregledu načrta. Obstaja seveda še četrti način, to je odkrivanje pomanjkljivosti pri dejanskem uresničevanju načrta, ki pa je iz razumljivih razlogov povsem nezaželen in je tu naveden bolj v svarilo.

Spremljanje sprememb v informacijskem sistemu v kombinaciji s testiranjem načrta je najprimernejši, na žalost pa tudi najtežji način ugotavljanja potrebe po spremembah v okrevalnem načrtu. Problem tega postopka je v tem, da se informacijski sistem organizacije navadno spreminja tako hitro, da je brez skrbne organizacije spremembam nemogoče slediti. Postopek je mogoče olajšati tako, da se jasno opredelijo področja, kjer bo zagotovo prihajalo do sprememb in jih je zato treba spremljati. Ta področja se med organizacijami nekoliko razlikujejo, tako rekoč povsod pa mednje sodijo na primer podatki, aplikacije, strojna oprema in osebje. Poleg tega lahko spremljanje sprememb olajša že sama zasnova okrevalnega načrta.

Če je ta zasnovan dovolj odprto in prožno, lahko prenese del sprememb v informacijskem sistemu tudi brez poznejšega prilagajanja.

5.2.2 Spreminjanje podatkov

Spreminjanje podatkov je stalnica v vseh informacijskih sistemih. Pri tem sta s stališča okrevalnih postopkov pomembni predvsem dve vrsti podatkovnih sprememb: naraščanje količine podatkov in s tem povezano tudi morebitno spreminjanje strojne opreme ter staranje oziroma arhiviranje podatkov, kar navadno pomeni prenos podatkov na drugačen pomnilniški medij.

Pri naraščanju količine podatkov je pomembno, kakšna je stopnja centraliziranosti podatkov v organizaciji. Če so vsi podatki – ali vsaj večina njih – shranjeni v centralni lokaciji, potem metoda za kopiranje vseh podatkov osrednjega pomnilniškega sistema na oddaljeno lokacijo samodejno poskrbi za naraščanje podatkov. To seveda velja, dokler se ne spreminja strojna platforma, na kateri se podatki hranijo.

Pri uporabi distribuiranih baz podatkov oziroma podatkov, ki se nahajajo na decentraliziranih podatkovnih strežnikih, je treba na prilagajanje okrevalnih postopkov bolj paziti, saj naraščanje podatkov navadno zahteva tudi dodatno strojno opremo. Kadar so za različne vrste podatkov predvidene različne okrevalne strategije, je treba poleg količine spremljati tudi vsebino podatkov, saj je treba nove podatke razvrščati v ustrezne skupine glede na način njihovega kopiranja.

Staranje podatkov v veliki večini primerov pomeni prenos podatkov na drug pomnilniški medij, navadno gre pri tem za prenos s hitrih diskov na trakove ali počasne diskovne medije. Pri tem nastane težava, saj se spremembe na hitrih diskovnih medijih prenašajo posamezno, za vsako datoteko posebej, medtem ko se spremembe na počasnih medijih navadno prenašajo agregatno, tako da se hkrati menja vsebina celotnega medijskega nosilca. Na ta problem je vsekakor treba paziti že pri zasnovi postopkov kopiranja podatkov, glede vzdrževanja načrta pa je pomemben v toliko, da je treba spremljati morebitne spremembe zastaralnih rokov za različne vrste podatkov in okrevalni načrt ustrezno prilagajati. Tudi v tem primeru je mogoče pri centraliziranih podatkih postopek vzdrževanja načrta močno olajšati, in sicer z uporabo katerega od komercialnih produktov za migracijo podatkov.

5.2.3 Spreminjanje aplikacij in strojne opreme

Naslednja pogosta sprememba v informacijskem sistemu je sprememba aplikacij, ki je navadno v dokaj tesni zvezi tudi s spremembo podatkov. Spreminjanje aplikacij je s stališča okrevalnih postopkov pomembno iz več razlogov. Korenitejša sprememba obstoječih,

predvsem pa uvajanje novih aplikacij navadno prinašata tudi spremembe pri strojni opremi, ki jih je treba upoštevati. Poleg tega potreba po spremembah aplikacij najpogosteje nastane zaradi spremenjene poslovne prakse, kar s sabo navadno prinaša še druge spremembe v topologiji informacijskega sistema, ki jih je treba upoštevati pri okrevalnem načrtu.

Sprememba strojne opreme v vsakem primeru prinaša tudi potrebo po spremembi okrevalnega načrta. Glede na to, da se strojna oprema najpogosteje spreminja na ravni končnih uporabnikov (delovne postaje, lokalni strežniki ipd.), je dobro poskrbeti, da je ta del načrta zasnovan bolj splošno, tako da ga je mogoče lažje spreminjati. Pogosto prinaša sprememba strojne opreme na lokalni ravni tudi spremembo operacijskega sistema, na kar je prav tako treba paziti.

5.2.4 Izvajanje informacijskih projektov v organizaciji

Svetovalna hiša Gartner v svojih analizah predlaga, da bi moralo zagotavljanje poslovanja postati sestavni del organizacijske kulture in da bi to področje moralo biti vsebovano v vsakem informacijskem razvojnem projektu. Zato predlaga, da bi bilo v različnih projektnih fazah treba opraviti naslednje analize oziroma dejavnosti (Witty, 2001 b):

- narediti analizo vpliva na poslovanje v okviru katere bi ugotovili pomembnost novega sistema za poslovanje organizacije in posledice njegovega morebitnega izpada,
- določiti ciljni čas vzpostavitve delovanja (RTO),
- določiti ciljno točko restavriranja podatkov (RPO),
- ugotoviti vpliv novega sistema na obstoječe sisteme v organizaciji,
- opredeliti možnosti alternativnega delovanja novega sistema, jih implementirati in ustrezno prilagoditi okrevalni načrt.

Dosledno upoštevanje navedenih pravil bi bistveno olajšalo spremljanje sprememb, ki se v informacijskem sistemu uvajajo s posameznimi projekti. Poleg tega je treba v organizaciji zagotoviti tudi nadzorovano opravljanje manjših posegov v informacijski sistem, ki sicer ne vplivajo pomembno na delovanje samega sistema, kot so na primer menjave lokalne strojne opreme ali zamenjava lokalnega telekomunikacijskega ponudnika. Tudi v takih primerih je treba ugotoviti, ali sprememba v čemer koli lahko vpliva na učinkovitost okrevalnih postopkov.

S spremembami okrevalnega načrta je treba seznaniti tudi vse člane in vodje okrevalnih ekip, saj nekatere spremembe lahko pomenijo tudi drugačno delovanje v kriznih situacijah. Poleg tega je treba spremljati tudi spremembe na kadrovskem področju. Odhodi članov okrevalnih ekip in njihova zamenjava z novimi sicer zahtevajo v okrevalnem načrtu le popravke v klicnih

listah, treba pa je paziti na to, da se novi delavci ustrezno usposobijo in pripravijo tudi za delo v izrednih razmerah, ker je še posebej pomembno pri zamenjavi vodij okrevalnih ekip.

5.2.5 Problem zunanjih izvajalcev

Posebno pozornost je treba nameniti tudi zunanjim izvajalcem, s katerimi ima organizacija podpisane pogodbe o izvajanju del. Že pri podpisovanju pogodb je treba paziti na to, da bo v njih opredeljena tudi odgovornost zunanjega izvajalca, kako bo izvajal svoj del obveznosti v izrednih razmerah. Pri tem je treba čim bolj natančno opredeliti vse potrebne elemente, s katerimi bo zagotovljena ustrezna raven storitve (Matlus, Maurer, 2002). V času sodelovanja je treba pogodbena zagotovila občasno preverjati in če pride do kakršnega koli odstopanja od pogodbenih zagotovil ali če se zahteve organizacije spremenijo, po potrebi poiskati alternativnega ali nadomestnega zunanjega izvajalca.

5.3 Testiranje okrevalnega načrta

5.3.1 Cilji testiranja

Testiranje okrevalnega načrta je obvezen sestavni del njegovega vzdrževanja. Splošni namen testiranja je ugotoviti, ali je mogoče z uresničevanjem okrevalnega načrta zagotoviti delovanje informacijskega sistema v želenem času in obsegu. Poleg splošnega pa ima testiranje še druge cilje (Toigo, 2000, str. 378):

- ***Kontrola načrta.*** S testiranjem načrta je mogoče odkriti njegove pomanjkljivosti in jih odpraviti. V tej funkciji testiranje omogoča tudi ugotavljanje neskladnosti načrta z dejanskim stanjem informacijskega sistema.
- ***Merjenje učinkov.*** Testiranje je edini način, s katerim je mogoče ugotoviti, koliko časa je potrebno za izvedbo njegovih posameznih faz in v kolikšnem času je mogoče ponovno vzpostaviti delovanje, seveda v optimalnih razmerah. Poleg tega je med testom mogoče izmeriti tudi zmogljivosti in učinkovitost nadomestnih zmogljivosti.
- ***Vaja.*** Testiranje je nujno potrebno za nabiranje izkušenj. Člani okrevalnih ekip morajo dobro poznati posamezne postopke in svoje vloge v njih, saj bodo le tako lahko v kriznih trenutkih svoje naloge opravljali hitro in usklajeno.

5.3.2 Način in pogostnost testiranja

Glede načina testiranja torej ni splošno veljavnih pravil, način je odvisen le od ciljev, ki se s testiranjem poskušajo doseči. Načrta se tako lahko testira ob vnaprej določenih terminih ali nenapovedano. Napovedani testi so varnejši, izvedeni so v kar najbolj optimalnih razmerah in

so primernejši za pridobivanje rutine, medtem ko nenapovedani testi lahko prikažejo bolj realno sliko učinka posameznih sodelujočih in učinkovitosti načrta v celoti. Testiranja se med sabo lahko razlikujejo tudi po obsegu, saj je mogoče izvesti vse postopke okrevalnega načrta ali pa le njegove posamezne faze.

Ne glede na izbrani način pa se je treba na testiranje pripraviti, da bi lahko dalo želene rezultate. Najbolj pomembno je, da je testiranje izvedeno natančno po postopkih okrevalnega načrta, brez improvizacij. Toigo priporoča še nekatere zahteve, ki morajo biti izpolnjene, da bi bilo testiranje okrevalnega načrta učinkovito (Toigo, 2000, str. 379-381).

- ***Vnaprej pripravljen scenarij testa.*** Vsak test mora imeti pripravljen scenarij izrednega dogodka, ki je predmet testiranja, na primer popolno uničenje osrednje lokacije, izpad prostranih povezav, uničenje pomnilniškega sistema ipd. V scenariju morajo biti opredeljene tudi morebitne privzete dodatne predpostavke, kot na primer trajanje izpada, odsotnost dela osebja ipd.
- ***Jasno določeni cilji testiranja.*** Cilji testiranja morajo biti določeni pred njegovim začetkom. Biti morajo jasni in merljivi, saj je le tako pozneje mogoče oceniti uspešnost testiranja, na primer čas, potreben za obveščanje in prihod izvajalcev, čas obnovitve prostranih povezav, učinkovitost nadomestnega računalniškega sistema ipd.
- ***Dokumentiranje rezultatov testiranja.*** Rezultati in opažanja med testiranjem morajo biti kolikor je mogoče natančno dokumentirani za poznejšo analizo. Dokumentirana morajo biti tudi morebitna odstopanja od načrta, do katerih je prišlo med testiranjem.

Podobno kot velja za način izvedbe, tudi glede pogostnosti testiranja ni posebnega pravila. Testiranja bi morala biti dovolj pogosta, da se ohranja stik s spremembami v informacijskem sistemu in da se vzdržuje poznavanje postopkov pri izvajalcih na primerni ravni. Pogostnost testiranja je tako odvisna od hitrosti spreminjanja informacijskega sistema organizacije in od želene ravni poznavanja izvedbe okrevalnih postopkov. Po drugi strani pa seveda velja, da testiranja motijo redni delovni proces in prinašajo dodatne stroške. Potrebe po testiranju se med organizacijami lahko močno razlikujejo, po izkušnjah pa bi moral biti popolni test izveden najmanj enkrat na leto, delni pa glede na potrebe pogosteje. Pri tem je treba upoštevati, da je vsak prenos delovanja na alternativni sistem v primeru načrtovanega izpada glavnega sistema zaradi vzdrževanja ali popravila lahko tudi odličen test, če je tak prenos narejen v skladu s prej navedenimi zahtevami za testiranje.

5.4 Skrbnik okrevalnega načrta

Za skrbništvo nad okrevalnim načrtom mora organizacija določiti skrbnika. Najprimerneje je, da je to oseba, ki je vodila ali vsaj pomembno sodelovala pri projektu uvajanja pogojev za zagotavljanje delovanja informacijskega sistema in izdelavi okrevalnega načrta. Njegov

položaj je sicer odvisen od organizacijske strukture v organizaciji, vendar mora biti dovolj visok, da ima dober pregled nad dogajanjem v celotnem informacijskem in telekomunikacijskem sistemu organizacije. Njegove naloge so:

- spremljanje sprememb v informacijskem sistemu organizacije,
- prilagajanje okrevalnega načrta,
- priprava, izvedba in analiza testiranja načrta,
- koordiniranje načrtovanega ali izrednega vzpostavljanja delovanja na alternativnem informacijskem sistemu.

Zaradi varnosti je treba skrbniku okrevalnega načrta določiti tudi namestnika, ki lahko ob njegovi morebitni odsotnosti koordinira vzpostavitev delovanja informacijskega sistema ob izrednem dogodku.

6 Sklep

Učinkovitost in uspešnost poslovanja sodobnih organizacij sta iz leta v leto bolj odvisni od kakovostne in nemotene informacijske podpore, pri čemer postajajo razlike med pridobitnimi, nepridobitnimi, velikimi in manjšimi organizacijami čedalje manjše. Zato imajo že krajši izpadi informacijskega sistema precejšnje posledice na poslovanje, medtem ko lahko dlje trajajoči izpad ali trajna izguba podatkov postavita obstoj organizacije na kocko. V primerih, da se kaj takega zgodi pri javnih institucijah, ima to lahko še mnogo širše negativne posledice, ki lahko v zelo kritičnih primerih resno ogrozijo delovanje in celo obstoj države.

Zato so v organizacijah na nekaterih področjih, kot so na primer bančništvo, vladne institucije, telekomunikacije ipd., začeli poslovne informacijske sisteme obravnavati kot kritično infrastrukturo, za katero je treba tudi z zakonsko regulativo zagotoviti ustrezno preventivno delovanje, katerega namen je zagotoviti varnost podatkov in delovanje informacijskega sistema v izrednih situacijah. Vendar pa se tudi pri organizacijah, ki sicer ne sodijo v katero od kritičnih področij, vse pogosteje uveljavlja prepričanje, da je treba nekako vzpostaviti možnosti za zagotavljanje informacijske podpore poslovanja, čeprav se problema marsikje lotevajo dokaj pomanjkljivo.

Pri zagotavljanju delovanja informacijskih sistemov se je v zadnjih desetih letih zgodil pomemben premik z razmišljanja o okrevanju sistema po nesreči (*disaster recovery*) proti zagotavljanju nadaljevanja poslovanja (*business continuity*). Vzrok za to je širitev informacijske podpore na čedalje širši segment poslovanja, zaradi česar so postali

informacijski sistemi tako zapleteni, da stari okrevalni postopki niso bili več primerni. S tem premikom se je tudi odgovornost za uvajanje rešitev začela seliti s tehničnega čedalje bolj na organizacijsko oziroma poslovno področje. Ker pomeni poslovni informacijski sistem bistveni povezovalni element poslovanja sodobne organizacije, je treba pripravo organizacije na nepredvidene dogodke začeti prav pri načrtu zagotavljanja delovanja njenega informacijskega sistema.

Prvi korak, ki ga je treba narediti, sta analiza tveganja in analiza vpliva na poslovanje. Z njima je treba ugotoviti, kakšne nevarnosti pretijo delovanju posameznih delov informacijskega sistema in kakšne posledice ima izpad posameznega dela in s tem posameznega poslovnega procesa na poslovanje organizacije. Ta korak je hkrati dobrodošla priložnost za pregled poslovnih procesov, oceno primernosti informacijske podpore in pregled obstoječih zaščitnih in varnostnih mehanizmov v organizaciji. Analizi sta pomembni, saj je prav od njunih izsledkov odvisno, v kakšnem obsegu, če sploh, se bodo ukrepi za zagotavljanje delovanja informacijskega sistema v organizaciji izvajali.

Preprečevanje izpadov je iz več razlogov primernejše kakor odpravljanje njihovih posledic, zato je preventivno delovanje eden pomembnejših ukrepov za zagotavljanje delovanja informacijskega sistema. Preventivne postopke bolj ali manj izvajajo vse organizacije, v analizi tveganja jih je treba le kritično ovrednotiti in po potrebi predlagati spremembe. Poleg fizične in logične zaščite sistema je treba nameniti precejšnjo pozornost tudi izobraževanju in osveščenosti zaposlenih, saj prav kakovost njihovega dela lahko prepreči največ nepričakovanih izpadov.

Ne glede na kakovost preventivnih postopkov pa ti ne morejo v popolnosti zagotoviti delovanja sistema, zato je potrebna tudi izdelava okrevalnega načrta, v katerem so opredeljeni postopki, s katerimi je mogoče v primernem času nadomestiti izpad primarnega informacijskega sistema z alternativnimi rešitvami. Temelj za izdelavo načrta je analiza tveganja, v kateri sta opredeljena ciljna točka restavriranja podatkov (*Recovery Point Objective - RPO*) in ciljni čas vzpostavitve delovanja (*Recovery Time Objective - RTO*) za posamezne poslovne aplikacije in njihove podatke. Na podlagi teh ciljnih točk se v načrtu opredelijo spleti okrevalnih postopkov za posamezne dele informacijskega sistema, ki zajemajo podatke, strojno opremo in telekomunikacijske povezave.

Ko je okrevalni načrt izdelan, mora organizacija določiti njegovega skrbnika. Naloga slednjega je spremljanje sprememb v informacijskem sistemu organizacije in ustrezno prilagajanje načrta. Prav tako mora skrbeti za usposabljanje članov okrevalnih ekip in redno testiranje postopkov.

V Sloveniji je raven zagotavljanja delovanja poslovnih informacijskih sistemov dokaj nizka. Iz splošnega povprečja nekoliko izstopa področje bančništva, kjer so zaradi sklepa Banke Slovenije o obveznem upoštevanju standarda ISO 17799 v zadnjih letih izpeljali nekaj

projektov, ki pa večinoma ne presegajo ravni kopiranja podatkov na oddaljene pomnilniške medije. Podobno velja tudi za slovensko državno upravo, kjer je vlada s svojim sklepom z dne 3. oktobra 2002 sicer sprejela priporočila Centra vlade za informatiko, vendar pa se resnejših projektov z izjemo policije niso lotili še nikjer.

V slovenski policiji je bila leta 2001 izdelana analiza razpoložljivosti njenega informacijskega sistema, ki je pokazala, da ta ne dosega standardov, ki jih predpisujejo določila Schengenskega sporazuma. Zato se je v začetku leta 2002 začel uresničevati projekt za vzpostavitev sekundarnega računalniškega centra in povezavo računalniških sistemov v obeh centrih s pomočjo arhitekture *Geographically Dispersed Parallel Sysplex*. Na ta način bo mogoče zagotoviti skoraj neprekinjeno delovanje informacijskega sistema policije tako ob načrtovanih kot nenadnih izpadih primarnega sistema. Projekt, ki naj bi se predvidoma končal leta 2005, je prvi tako temeljit primer reševanja tovrstne problematike v Sloveniji.

Uvajanje pogojev za zagotavljanje delovanja poslovnega informacijskega sistema nikakor ni ne lahka, ne poceni naloga. Vendar pa se je treba zavedati, da sta trajna izguba podatkov ali daljša prekinitev poslovanja zaradi izpada informacijske podpore za organizacijo lahko še neprimerno dražji, v nekaterih bolj izpostavljenih primerih pa tudi usodni.

7 Literatura in viri

Literatura

1. Boroski Doran: Protect Processes As Well As Investments In Disaster recovery Plans. Computerworld, vol. 36 (2002), št. 11, str. 17.
2. Calvert Michael: A Site Selection Checklist for Moving Your Data Center. Inside Gartner This Week, vol 17 (2001), št. 44, str. 9, 10.
3. Calvert Michael: Disaster Recovery Needs Document Management. Inside Gartner This Week, vol 18 (2002), št. 7, str. 10-12.
4. Everett Cath: When the worst happens. IT today, Computerweekly publication, 20.4.2002, str. 24, 25.
5. Fulmer Kenneth L.: Business Continuity Planning. Brookfield, Connecticut, Rothstein Associates Inc., 2000, 134 str.
6. Girard John: CIO Alert: The »Last Mile« Is Critical in Network Disaster Resilience. Gartner article IGG-09182002-02, 18.9.2002
7. Hall Mark: IT Watchfulness Rises, But Budgets Limit Change. Computerworld, vol. 36 (2002), št. 37, str. 6.
8. Hoffman Thomas: Economy caps Security Spending. Computerworld, vol. 36 (2002), št. 37, str 48.
9. Kreizmann Gregg, Mingay Simon: Top Concerns of Government Business Continuity Planners. Gartner research QA-13-5355, 19.6.2001
10. Kun Maria, Furlonger David: Resiliency Lessons: NYSE, the Amex, Electronic Exchanges. Gartner research COM-15-6359, 14.3.2002
11. Levitt Alan M.: Disaster Planning and Recovery: a guide for facility professionals. New York, NY, John Wiley & Sons, 1997, 417 str.
12. Logan Debra: A Secure, Resilient Enterprise Needs Content Management. Gartner research TG-15-8647, 14.3.2002
13. Malik William: A Proces Approach to Business Continuity Planning. Gartner research COM-14-5299, 2.10.2001
14. Matlus Richar, Maurer William: Add Security and Business Continuity to Sourcing Contract. Gartner research DF-15-1089, 18.3.2002
15. Mayer Kenneth M.: Manager's guide to Contingency Planning for Disasters: protecting vital facilities and critical operations, 2 .izdaja. New York, NY, John Wiley & Sons, 1999, 234 str.
16. Mingay Simon: Disaster Recovery Reciprocal Agreement Returning. Gartner research SPA-15-9792, 12.4.2002
17. Neil David: Anticipate the Need for Resilience: One Company That Did. Gartner research CS-14-9815, 18.12.2001
18. Nicolett Mark: Distributed vs. Centralized Infrastructure for Resilience. Gartner research DF-14-5547, 14.12.2001

19. Noakes-Fry Kristen, Diamond Trude: Business Continuity and Disaster Recovery Planning and Management: Perspective. Gartner research DPRO-100862, 8.11.2001
20. Noakes-Fry Kristen, Diamond Trude: Business Continuity Planning Software: Perspective. Gartner research DPRO-100469, 22.2.2002
21. Scott Donna: Data Centers: Optimal Distances for Disaster Recovery. Gartner research DF-14-9811, 14.12.2001
22. Scott Donna, Browning James: Preparing for a Disaster: Affordable SMB Actions. Gartner research COM-15-1408, 6.3.2002
23. Scott Donna, Gassman Bill: The Ripple Effect: Disaster's Indirect Impact. Gartner research TG-14-5298, 20.11.2001
24. Scott Donna, Krischer Josh: Real-Time Enterprise: Business continuity and Availability. Gartner research SPA-18-1638, 24.9.2002
25. Scott Donna, Krischer Josh, Rubin Jon: Disaster Recovery: Wighing Data Replication Alternatives. Gartner research T-13-6012, 15.6.2001
26. Scott Donna, Witty Roberta: E-Business Continuity; 'You've Come a Long Way Baby!'. Gartner research COM-13-6392, 18.6.2001
27. Tate Jon et al.: Introduction to SAN Distance Solutions. IBM Redbooks, 2002, 476 str.
28. Toigo Jon William: Disaster Recovery Planning: for computer and communication resources. New York, NY, John Wiley & Sons, 1996, 329 str.
29. Toigo Jon William: Disaster Recovery Planning: strategies for protecting critical information, 2. izdaja. Upper Saddle River, New Jersey, Prentice Hall PTR, 2000, 432 str.
30. Verton Dan: Disaster Recovery Planning Still Lags. Computerworld, vol. 36 (2002), št. 14, str. 8.
31. Verton Dan: Corporate America Now on Front Lines of War on Terror. Computerworld, vol. 36 (2002), št. 37, str. 7.
32. Wheatman Vic: Aftermath: Disaster Recovery. Gartner research AV-14-5238, 21.9.2001
33. Witty Roberta et al.: The Price of Information Security. Gartner research R-11-6534, 8.6.2001
34. Witty Roberta: What Is Crisis Management? Gartner research TU-14-5246, 19.9.2001
35. Witty Roberta: Building Business Continuity Planning Into Every IT Project. Gartner research TU-14-9813, 18.12.2001
36. Younker Edward: How Effective Is Your Crisis management Plan? Inside Gartner This Week, vol 17 (2001), št. 39, str. 4-6.
37. Younker Edward: Elements of Successful IT Risk Management Program. Inside Gartner This Week, vol 18 (2002), št. 6, str. 1-6.

Viri

1. BCP Comes of Age: intervju Information Security Magazine [URL: http://www.rothstein.com/articles/bcpage.html], 8.11.2002
2. Center Vlade RS za informatiko: Priporočila za pripravo informacijske varnostne politike [URL: http://www.gov.si/cvi/], 3.2.2003
3. Computer Science and Telecommunication Board: Cybersecurity Today and Tomorrow: Pay Now or Pay Later [URL: http://stills.nap.edu/html/cybersecurity], 25.1.2002
4. Eagle Rock Alliance: 2001 Cost of Downtime [URL: http://www.contingencyplanningresearch.com], 16.2.2003
5. Geographically Dispersed Parallel Sysplex: the S/390 Multi-site Application Availability Solution. IBM GF22-5063-00, 1998.
6. Hiles Andrew: Business Impact Analysis: What's Your Downside? [URL: http://www.rothstein.com/articles/busimpact.html], 19.9.2002
7. Karta makroseizmičnih intenzitet [URL: http://www.sigov.si/ugf/ang/hazard/intenz.gif], 15.10.2002
8. Poplavne površine [URL: http://ufp-si.eionet.eu.int/ewnsi/index.htm], 15.10.2002
9. Rihar Boštjan, Turk Marjan: Razpoložljivost informacijskega in telekomunikacijskega sistema policije. Gradivo za interno uporabo, junij 2001
10. Rothstein Philip J.: September 11 Changes Everything [URL: http://www.rothstein.com/articles/sept11.html], 8.11.2002
11. The SANS Institute: The Twenty Most Critical Internet Security Vulnerabilities [URL: http://www.sans.org/top20/], 8.11.2002
12. Sklep o določitvi pogojev, ki jih mora izpolnjevati banka oz. hranilnica ... (Uradni list RS, št. 52/2000)
13. Urad vlade za informiranje Republike Slovenije: Priporočila za pripravo informacijske varnostne politike.Sporočilo za javnost o sklepih, ki jih je Vlada RS sprejela na 91.seji, 3. oktobra 2002 [URL: http://www.gov.si/cvi/], 3.2.2003

8 Priloga

Slovar uporabljenih kratic

ATM	Asynchronous Transfer Mode Asinhroni prenosni protokol izmenjave podatkov v prostranem omrežju
CE	Channel Extender Naprava za povezovanje IBM centralnih računalnikov s periferijo preko prostranega omrežja
DWDM	Dense Wavelength Division Multiplexer Valovno multipleksiranje optičnih signalov
E3	G.751 E3 prenosni standard mednarodne telekomunikacijske zveze
GDPS	Geographically Dispersed Parallel Sysplex IBM arhitektura za povezovanje dveh centralnih računalnikov z namenom zagotavljanja delovanja informacijskega sistema
ISDN	Integrated Services over Digital Network Digitalno omrežje za prenos podatkov in govora
ITSP	Informacijsko Telekomunikacijski Sistem Policije
NAS	Network Attached Storage Diskovno polje priključeno na lokalno omrežje
RAID	Redundant Array of Independent Disks Polje redundantnih diskovnih podatkovnih nosilcev
RPO	Recovery Point Objective Ciljna točka restavriranja podatkov
RTO	Recovery Time Objective Ciljni čas vzpostavitve delovanja informacijskega sistema
S/390	System 390 Vrsta IBM centralnih računalnikov
SA	System Automation Programska oprema IBM za avtomatizacijo sistemskih posegov
SAN	Storage Area Network Omrežje za shranjevanje podatkov
SDH	Synchronous Digital Hierarchy Sinhroni prenosni protokol izmenjave podatkov v prostranem omrežju

SDM	System Data Mover Programska oprema IBM za asinhrono kopiranje podatkov
SLA	Service Level Agreement Dogovor o ravni storitev
TCP/IP	Transmission Control Protocol/Internet Protocol Prenosni protokol v internetnem omrežju
UPS	Uninterruptible Power Supply Naprave za zagotavljanje neprekinjenega napajanja
XRC	Extended Remote Copy IBM Asinhroni način kopiranja podatkov