UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

D I P L O M S K O D E L O

OKREVANJE INFORMACIJSKIH SISTEMOV PO NESREČAH

Ljubljana, september 2004 GREGOR ZORČ

IZJAVA

Študent Gregor Zorč izjavljam, da sem avtor tega diplomskega dela, ki sem ga napisal pod mentorstvom dr. Jurija Jakliča, in dovolim objavo diplomskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne_____ Podpis: _____

Kazalo

1 Uvod

Informacijska tehnologija ter načrtovanje, namestitev in upravljanje informacijskih sistemov organizacij postajajo osnovna infrastrukturna in operativna nujnost vseh podjetij in vseh panog. Ker je poslovanje organizacij vse bolj odvisno od informacijskega sistema, je potrebno v same informacijske sisteme vgraditi tudi varnostne mehanizme, ki preprečujejo zaustavitev poslovanja zaradi napak, sesutij in prekinitev v informacijskem sistemu. Nepravilno delovanje informacijskega sistema lahko povzroči znižanje nivoja storitev ali celo izgubo poslov, če je stopnja nedelovanja informacijskega sistema prevelika ali če nedelovanje traja predolgo. Bančni sektor, na primer, je izredno odvisen od informacijskega sistema. Kadar se pojavi večja napaka v informacijskem sistemu, je lahko celotno poslovanje banke ustavljeno. Med poslovno najbolj očitnimi negativnimi posledicami takšnih napak so: izguba dobička, izguba ugleda organizacije, zmanjšanje konkurenčnih prednosti organizacije ter izguba tržnega deleža (Chow, 2000, str. 80).

Kvaliteta odločitev, ki so sprejete med krizno situacijo, je v večini primerov dosti nižja od tistih, ki so sprejete v okoliščinah, ko je na voljo dovolj časa za razmislek o vseh možnostih. Načrtovanje okrevanja po nesrečah (angl. disaster recovery planning) mora zato postati nujnost za organizacije, katerih poslovanje je močno odvisno od informacijskega sistema, saj jim lahko pomaga zmanjšati izgube, ki nastanejo ob nesrečah. Vnaprejšnja izdelava in preizkus načrta ob nesrečah je najpomembnejši element pomoči za preživetje organizacij, ki jih je doletela nesreča.

V nadaljnjem besedilu so predstavljene možnosti, ki jih imajo organizacije na razpolago pri pripravah v primeru nesreče. Namen diplomskega dela je predstaviti različne načrte in tehnične rešitve, ki podjetju omogočajo nadaljevanje poslovanja v primeru delnega ali celotnega poškodovanja informacijskega sistema. Poudarek je predvsem na načrtu okrevanja po nesrečah, na kratko pa so obravnavane tudi druge vrste načrtov. Pri načrtovanju okrevanja po nesrečah izmenično uporabljam pojma "načrtovanje" in "načrt". Oba se nanašata na načrtovanje okrevanja po nesrečah, le da je enkrat poudarek na načrtu kot dokumentu, drugič pa na dejavnosti načrtovanja.

Poleg proučevanja okrevanja po nesrečah s tehničnega vidika pa želim v diplomskem delu tudi pokazati, kakšno je trenutno dejansko stanje na tem področju. Predvsem me zanima delež organizacij, ki imajo pripravljen načrt okrevanja po nesrečah in ali ti načrti obsegajo varovanje informacijskega sistema v celoti ali samo deloma. Na podlagi tega so na koncu diplomskega dela podane ugotovitve o tem, kaj bi bilo treba še storiti na tem področju in kakšna bo vloga načrtovanje okrevanja po nesrečah v prihodnosti.

2 Načrtovanje okrevanja po nesrečah

Izraz "načrtovanje okrevanja po nesrečah" je v literaturi opisan na več različnih načinov. Hutt in drugi (Chow, 2000, str. 80) so načrtovanje okrevanja po nesrečah definirali kot skrb za računalniško

varnost za zagotovitev alternative organizacijam, ki se soočajo z naključnimi dogodki, ki bi lahko bili škodljivi za normalno delovanje organizacije. Rosenthal in Sheinink (Chow, 2000, str. 80) sta načrtovanje okrevanja po nesrečah definirala kot ureditev poslovnih operacij v sili ter operacij podatkovnega centra v sili, skupaj z načrtovanjem okrevanja, ki sledi nesreči. Drugi avtor, Paradine (Chow, 2000, str. 80), načrt okrevanja po nesrečah definira kot načrt, ki omogoča obnovitev stanja, kakršno je bilo pred nesrečo, če organizacija utrpi večjo škodo ali če jo prizadene kakšen drug razdejalen dogodek. Yiu in Tse (Chow, 2000, str. 81) pa sta definirala načrtovanje okrevanja po nesrečah kot postopke, ki se uporabljajo za zagotavljanje okrevanja ustreznih informacij, v časovnem roku nedelovanja sistema, ki si ga lahko organizacija še privošči, ko se zgodi nesreča.

Tudi pojem "nesreča" različni avtorji definirajo različno. Snoyer in Fischer (Chow, 2000, str. 80) sta pojem "nesreča" (angl. disaster) definirala kot: "dogodek, ki zelo verjetno povzroči velik razdor v delovanju organizacije za neko časovno obdobje." Arnell (Chow, 2000, str. 80) je po drugi strani definiral nesrečo kot "vsak dogodek, ki lahko povzroči velik razdor v zmožnosti delovanja informacijskega sistema za neko časovno obdobje in vpliva na delovanje organizacije." Po njegovem mnenju je namen načrtovanja okrevanja po nesrečah minimiziranje finančnih izgub, vzdrževanje neprekinjenosti poslovanja, zagotavljanje integritete podatkov ter pravočasna in časovno učinkovita obnovitev običajnih operacij.

2.1 Zgodovina

V šestdesetih in sedemdesetih letih devetnajstega stoletja so začeli upravljavci informacijskih sistemov opažati, da postajajo njihovi sistemi posamezna točka napake[1] (angl. single point of failure). Napake, ki so se pripetile v informacijskem sistemu, so lahko imele velik vpliv na delovanje drugih delov organizacije, od otežkočenega poslovanja do popolne ustavitve poslovanja. V tem času so bili informacijski sistemi, vključno z omrežnimi povezavami, polni posameznih točk napak.

V tistem času so strokovnjaki za informacijsko tehnologijo znali razviti informacijske sisteme, ki so bili dovolj prilagodljivi, da v njih ni bilo več posameznih točk napak. Delujoči primerki takšnih sistemov so bili razviti za vladne organizacije, raziskovalne organizacije in vojsko. Eden prvih IBM-jevih osrednjih računalnikov, System 360 Model 67, je imel na voljo izvedenko z dvema procesorjema, kar je povečalo zanesljivost delovanja. Sistemi, ki so v tem času poganjali Bell-ove telefonske centrale, so bili tudi platforme z visoko razpoložljivostjo.

[1] Točka (naprava, programska oprema, telekomunikacijska poveza ipd.) v sistemu, za katero ni na voljo nobena nadomestitev. Če se zgodi napaka v takšni točki, potem sistem ne deluje več popolno. Posamezne točke neuspeha se ne sme zamenjati s sistemom, ki lahko odpove samo v eni točki. Posameznih točk neuspeha je namreč lahko v enem sistemu več (Herman, Neumeier, 2004).

Povprečna organizacija si v tistem času ni mogla privoščiti drage tehnologije, da bi odstranila svoje posamezne točke napak. Vendar pa je bila potreba po alternativnih rešitvah prisotna in je rasla, saj je poslovanje organizacij postajalo vse bolj odvisno od računalniške tehnologije.

Na koncu 70-ih let so začeli dobavitelji ponujati deljen dostop do okolij za obnovitev računalniških procesov. Stroški takšnega najema so bili občutno manjši, kot če bi morala organizacija sama podvojiti vso opremo, na kateri tečejo njene kritične aplikacije. Čeprav na ta način posameznih točk napak niso povsem odstranili, pa je zaradi stroškovno učinkovite rešitve ta način postal standarden v poslovanju takratnega časa.

2.2 Zveza med načrtovanjem okrevanja po nesrečah in načrtom neprekinjenega poslovanja

Načrt neprekinjenega poslovanja je lahko izdelan za določen poslovni proces ali pa tudi za vse kritične poslovne procese. Načrt neprekinjenega poslovanja je krovni dokument, katerega pomemben del je tudi dokument načrtovanje okrevanja po nesrečah. Informacijski sistemi so v načrtu neprekinjenega poslovanja obravnavani samo v vlogi podpore obravnavanim poslovnim procesom. Načrt neprekinjenega poslovanja se sestoji iz naslednjih glavnih načrtov:

- načrt obnovitve poslovanja,
- načrt zaščite in reševanja,
- načrt ravnanja ob incidentih,
- načrt neprekinjenega delovanja in
- načrt okrevanja po nesrečah.

Načrt obnovitve poslovanja, načrt zaščite in reševanja ter načrt neprekinjenega delovanja se ne ukvarjajo z informacijsko tehnologijo. Načrt ravnanja ob incidentih se ukvarja z informacijsko tehnologijo, in sicer uvaja postopke in navodila, kako ravnati ob napadih iz omrežij. V splošnem načrt ravnanja ob incidentih ne vključuje uporabe načrta okrevanja po nesrečah.

2.3 Drugi pristopi

Drugi avtorji predlagajo drugačne pristope k upravljanju nesreč in prekinitev v organizacijah. Tabela 1 prikazuje pristop Steva Davisa (2003), ki je razvil Splošen vodstveni načrt za izredne razmere.

Tabela 1: Komponente splošnega vodstvenega načrta za izredne razmere

Splošen vodstveni načrt za izredne razmere	Ublažitev	Okrevanje po nesrečah	Neprekinjeno poslovanje	Obnovitev poslovanja	Načrtovanje možnosti
Cilj	prepreči ali zmanjšaj vpliv	kritične računalniške aplikacije	kritični poslovni procesi	obnova procesov	alternativne rešitve
Fokus	preventiva	obnovitev podatkov	obnovitev procesov	vrnitev na običajno stanje	naredi, da bo delovalo
Primer dogodka	razlitje vode	napaka v strežniku	poplava v laboratoriju	požar v zgradbi	nedelovanje aplikacije
Rešitev	pregled ventilov	okrevanje na vroči lokaciji	posušitev in ponovni zagon poslovanja	nova oprema, nova stavba	uporabi ročni postopek

Vir: Davis, 2003.

2.4 Vrste nevarnosti

Večina strokovnjakov s področja načrtovanja okrevanja loči nevarnosti na tri skupine:

- naravne oz. okoljstvene nevarnosti,
- tehnične oz. mehanične nevarnosti,
- človeške aktivnosti in nevarnosti.

Tabela 2.: Vrste nevarnosti.

Naravne oz. okoljstvene nevarnosti	Tehnične oz. mehanične nevarnosti	Človeške aktivnosti in nevarnosti
požar	prekinitev dobave energije	računalniška napaka
poplava	uhajanje plina	izgubljeni/založeni dokumenti in datoteke
orkan	nedelovanje programske opreme	vandalizem
potres	problemi s kanalizacijo	kraja
udar strele	napake v zgradbi	grožnje z bombo
tornado, nevihta	nepravilna električna napeljava	neredi
sneg in snežne nevihte	razlitje strupov	stavka
veter	radioaktivno onesnaženje	ugrabitev
valovanje plime	izguba fizičnega dostopa do sredstev	terorizem
vrtinčast vihar (tajfun)	biološko onesnaženje	sabotaža
plesen in vlaga	iztirjenje vlaka	izguba ključnega osebja
insekti in glodalci	trčenje letala	epidemija

Vir: Rike, 2003, str. 26.

Nevarnosti oz. nesreče je potrebno razvrstiti tudi glede na njihov obseg vpliva. Nesreče z največjim obsegom delovanja zajamejo celotno populacijo nekega območja. Primeri takšnih nesreč so potresi, poplave, izpad celotnega električnega omrežja itd. Takšne vrste nesreč vplivajo na veliko število organizacij, ne samo na eno. Po drugi strani pa lahko nesreče vplivajo na manjše število organizacij, npr. eno ali nekaj. Primeri takšnih nesreč so npr. puščanje strehe na poslovni stavbi, lokalni požar itd.

2.5 Koristi in stroški načrtovanja okrevanja po nesrečah

Vodilni delavci v organizacijah se morajo zavedati koristi in stroškov načrtovanja okrevanja po nesrečah, preden se odločijo za implementacijo v podjetju. Spodaj so naštete koristi in stroški načrtovanja okrevanja po nesrečah.

2.5.1 Koristi implementacije načrtovanja okrevanja po nesrečah

Implementacija načrtovanja okrevanja po nesrečah pomeni izdelavo načrta, ki pomaga organizaciji pri obnovi svojega stanja v primeru izgube podatkov ali uničenja strojne opreme. Koristi so sledeče (Hawkins, Yen, Chou, 2000, str. 223):

Odstranitev zmede in napak
Z organizacijo odzivne skupine in delegiranjem dela na to skupino se lahko vodilni delavci posvetijo drugim kritičnim obveznostim med postopkom okrevanja po nesreči. Druge obveznosti vodilnih delavcev lahko vključujejo: vodenje odnosov z javnostmi, urejanje odnosov s strankami, nabava, prodaja, potrebe po dodatnih kadrih, pravne zadeve itd.

Zmanjšanje motenj v delovanju organizacije
Ker je odzivna skupina pripravljena ter je nadomestna lokacija na voljo v najmanjšem možnem času, se lahko delujoč sistem hitro vzpostavi ter tako čim bolj zmanjša prekinitev delovanja poslovnega procesa organizacije.

Izbira med alternativnimi rešitvami
Ker se načrt okrevanja po nesrečah izdeluje, preden se zgodi nesreča, imajo vodilni delavci dovolj časa, da preučijo vse možne rešitve. Tako določijo najboljše možne alternativne rešitve, ki jih lahko v primeru nesreče hitro izberejo glede na nastalo situacijo.

Zmanjšanje odvisnosti od ključnih zaposlenih
Če bi bila naloga ponovne vzpostavitve omrežja določena samo eni osebi ter bi bila ta oseba poškodovana med nesrečo, potem bi imela organizacija velike probleme pri ponovnem vzpostavljanju omrežja v najmanjšem možnem času. Zato se lahko v načrtu okrevanja po nesrečah

določi za vse ključne osebe, ki naj bi sodelovale pri ponovni vzpostavitvi omrežja, njihove namestnike. Tako lahko v primeru, da prva oseba ni na voljo, delo opravi njen namestnik.

Varovanje podatkov organizacije
Podatki so en najpomembnejših virov organizacije. Podatki so shranjeni v mnogih različnih oblikah: baze podatkov, besedilne datoteke, preglednice, multimedijske datoteke ipd. Podatki, ki so pomembni za organizacijo, so lahko: poštni seznami, poštni predali uporabnikov, baze podatkov, finančni dokumenti, prejeti in izdani računi, nabavnice, prejemnice itd. Večina teh podatkov se lahko hrani v digitalni obliki, največkrat na enem od sledečih medijev: magnetni diski, optični diski, magnetni trakovi itd. Med izdelavo načrta okrevanja po nesrečah se preveri tudi primernost trenutnih medijev, na katere organizacija shranjuje svoje podatke, ter se odpravi pomanjkljivosti, npr. zamenja izrabljene magnetne trakove, premesti medije v primerne prostore itd.

Zagotovitev varnosti osebja
Če se med nesrečo poškoduje poslovna stavba, je potrebno preseliti pisarne. Načrt okrevanja po nesrečah lahko vključuje ustanovitev posebne skupine, ki je odgovorna za preskrbo podpore zaposlenim v takšnih primerih.

Pomoč pri pravilnem okrevanju
Načrt okrevanja po nesrečah pokriva večino problemov, ki nastanejo ob nesrečah, ter zanje preskrbi tudi rešitve. Tako se lahko vodilni delavci posvetijo drugim (nepredvidenim) problemom, ki se pojavijo ob nesrečah, predvidene probleme pa rešuje drugo osebje organizacije.

2.5.2 Stroški implementacije načrtovanja okrevanja po nesrečah

Izdelava načrta okrevanja po nesrečah ni preprosta. Da bi bila uspešno izvedena, mora uporabiti različne vire organizacije. Pri implementaciji se pojavljajo razni stroški, med najpomembnejšimi so naslednji:

Stroški priprave načrta okrevanja po nesrečah
Vodilni delavci porabijo veliko časa, da določijo, kateri poslovni procesi so kritični in jih je potrebno obnoviti po nesreči. Ta proces lahko stane organizacijo veliko delovnih dni. Če pa se organizacija odloči, da ji bo načrt okrevanja po nesreči izdelal zunanji sodelavec oz. drugo podjetje, so stroški še višji. Iziv pri izdelavi načrtovanja okrevanja po nesrečah je prepričati vodilne delavce, da se naložba vanj izplača.

Stroški virov organizacije
Izvedba načrtovanja okrevanja po nesrečah je velika obveza za osebe, ki ga uvajajo v organizacijo. Izvedba načrta okrevanja po nesrečah potrebuje podporo vodilnih delavcev, sodelovanje zaposlenih na nižjih ravneh ter dostop do inventarja vseh kritičnih sredstev organizacije.

Stroški dodatne opreme
Prav tako lahko predstavlja velik strošek za organizacijo nakup dodatne opreme, ki je potrebna za izvedbo načrta okrevanja po nesrečah. Med takšno opremo sodijo podvojena strojna in programska oprema, dodatna oprema za izdelavo varnostnih kopij, rezervna lokacija itd.

2.6 Pogoji uspešnosti načrtovanja okrevanja po nesrečah

Za uspešno izvedbo in vzdrževanje načrtovanja okrevanja po nesrečah, mora biti izpolnjenih več pogojev. Spodaj so navedeni in na kratko opisani glavni pogoji, ki so našteti v različnih literaturah. Seznam je povzet po Chowu (2000, str. 81).

Podpora vodstva organizacije
Načrtovanje okrevanja po nesrečah je dolgoročna načrtovalna aktivnost, ki zahteva velik kapitalski vložek organizacije. Samo če vodstvo organizacije podpira izvedbo, se lahko dolgoročno zagotovi vire in finančno podporo potrebne za izdelavo, vzdrževanje in preizkušanje načrta okrevanja po nesrečah.

Zadostna finančna podpora
Največja ovira pri uvedbi načrtovanja okrevanja po nesrečah so stroški, ki so povezani z izdelavo, vzdrževanjem in preizkušanjem le-tega. Razlog za to je, da so stroški izdelave domnevno previsoki ter da projekt načrtovanja okrevanja po nesrečah ne prinese takojšnih prihodkov iz investicije. Zaradi tega je potrebno zagotoviti zadostno finančno podporo projektu, če želi organizacija uspešno uvesti načrtovanje okrevanja po nesrečah v svoje poslovanje. Zadostna finančna podpora omogoči, da se vpelje načrt okrevanja po nesrečah v takšni obliki, kot je bilo določeno v prvi fazi njegovega življenjskega cikla – v fazi načrtovanja.

Uskladitev ciljev načrta okrevanja po nesrečah s cilji organizacije
V začetni fazi načrtovanja okrevanja po nesrečah je potrebno definirati cilje, ki so skladni z cilji organizacije. Cilji načrtovanja okrevanja po nesrečah lahko služijo za osnovno vodilo pri izdelavi načrta, ki deluje in je skladen z nameni vodstva organizacije. S tem se izognemo izdelavi načrta, ki bi se oddaljil od svojega namena.

Vpeljava tehnik projektnega vodenja
Delovni načrt in urnik morata biti izdelana za upravljanje s procesi, ki so potrebni za izdelavo načrta okrevanja po nesrečah. Namen tehnik projektnega vodenja je točna določitev projektnih nalog, rokov za njihovo dokončanje, oseb odgovornih za dokončanje projekta, časovne razporeditve nalog, proračuna za vsako od nalog itd. Tako se lahko zagotovi, da bo projekt dokončan v predvidenem roku in s predvidenimi sredstvi.

Prisotnost formalne komisije za načrtovanje okrevanja
Vodstvo podjetja mora določiti komisijo za načrtovanje okrevanja, saj nekateri deli načrtovanja okrevanja po nesrečah vplivajo na več organizacijskih enot v organizacijah ter sta zato potrebna komunikacija in usklajevanje med oddelki. Dobro je, če ima ta komisija tudi formalno avtoriteto in odgovornost za vpeljavo projekta v vse oddelke.

Sodelovanje predstavnikov iz vseh oddelkov
Predstavniki iz vseh oddelkov organizacije morajo sodelovati v formalni komisiji za načrtovanje okrevanja, saj le ti najbolje poznajo delovanje in značilnosti svojih oddelkov.

Vključitev zunanjih svetovalcev
Določitev zunanjih svetovalcev je pomembna za integriteto celotnega načrta. Zunanji svetovalci pri reviziji načrtovanja okrevanja po nesrečah lahko odkrijejo napake, ki zaposlenim v organizaciji največkrat ostanejo skrite. Kombinacija vključitve zaposlenih v organizaciji ter zunanjih svetovalcev je pogosto uspešna, saj se tako vključi zunanje strokovno znanje v izdelavo načrta okrevanja po nesrečah.

Ocena tveganja in analiza vpliva
Načrt okrevanja po nesreči mora biti narejen za vsako organizacijo posebej ter prilagojen le njej. Da bi bil načrt okrevanja po nesreči stroškovno učinkovit, je treba pred izbiro strategij obnovitev narediti oceno tveganja in analizo vpliva. Ocena tveganja upošteva vse možne grožnje za informacijski sistem: naravne nesreče, odpoved strojne opreme, odpoved programske opreme in človeške napake. Analiza vpliva oceni posledice nesreče v informacijskem sistemu na delovanje posameznih oddelkov organizacije ter oceni najdaljše dovoljeno prekinitev delovanja informacijskega sistema. Vodstvo podjetja mora na podlagi ocene tveganja in analize vpliva oceniti ranljivost poslovanja organizacije ter nato določiti, koliko sredstev se bo namenilo za izdelavo varnostnih kopij informacijskega sistema in to na kakšen način.

Določitev najdaljše dovoljene prekinitve delovanja informacijskega sistema
Vodstvo organizacije bo lažje odobrilo višino sredstev, potrebnih za izdelavo in vzdrževanja sistema za okrevanje, če bo imelo podatke o najdaljši dovoljeni prekinitvi delovanja informacijskega sistema (oz. njegovih delov). Prav tako ti podatki pomagajo vodstvu pri izbiri sistemov za okrevanje, ki omogočajo obnovitev v prej določenih časovnih okvirih. Če organizacija ve, kakšna je njena najdaljša dovoljena prekinitev delovanja informacijskega sistema, se s tem izogne prevelikim (oz. premajhnim) investicijam v naprave za obnovitev delovanja.

Določitev prioritete aplikacij
Vse aplikacije v informacijskem sistemu niso enako pomembne in občutljive na motnje. Zaradi tega se v načrtu okrevanja določi stopnje zavarovanosti aplikacij ter se te stopnje določi za vsako aplikacijo posebej. Zaradi visokih stroškov nabave in vzdrževanja podvojene strojne in programske opreme pa tudi osebja je treba določiti prioritete aplikacijam. Določitev prioritet mora temeljiti na

kriteriju, koliko posamezna aplikacija vpliva na zmožnost organizacije, da normalno posluje. Aplikacijam, ki so nujno potrebne za delovanje organizacije, se določi najvišjo prioriteto.

Hranjenje na oddaljeni lokaciji

Hranjenje varnostnih kopij, rezervne strojne opreme, rezervne programske opreme, kopij navodil in dokumentacije je ključni del učinkovitega načrtovanja okrevanja po nesreči, saj omogoča organizaciji obnovitev potrebnih podatkov v primeru nesreče. Oddaljena lokacija mora biti geografsko dovolj oddaljena od primarne lokacije organizacije, tako da se verjetnost prizadetosti obeh lokacij zaradi iste nesreče zmanjša na najmanjšo možno vrednost. Pri oddaljeni lokacije pa je treba določiti tudi ustrezni transportni sistem za fizično opremo in podatke do oddaljene lokacije in nazaj.

Prisotnost postopkov za primer nesreče

Postopki za primer nesreče so skupek navodil, kako ravnati takoj po nesreči. Ti postopki so kritični, saj je od ukrepov takoj po nesreči odvisno, koliko časa bo trajala prekinitev delovanja informacijskega sistema. Celotno osebje mora vedeti, kdo je odgovoren za katero področje ter katera dejanja se od njega pričakujejo v primeru nesreče. Postopki pa morajo biti podani jasno, da so razumljivi celotnemu osebju.

Urjenje osebja

Člani skupine za okrevanje morajo razumeti dodeljene naloge, ter morajo biti ustrezno izurjeni. Ključno osebje mora neprestano obnavljati znanje, saj se postopki v načrtu okrevanja po nesreči neprestano spreminjajo. Le tako bodo lahko člani skupine za okrevanje v primeru nesreče lahko samostojno reševali probleme, ki v takšnih primerih nastanejo.

Primerna rezervna lokacija

Izbira primerne rezervne lokacije za informacijski sistem je nujna, saj je lahko v primeru nesreče primarna lokacija neuporabna. Organizacija lahko izbira med različnimi tipi rezervnih lokacij: vroče lokacije, hladne lokacije, mobilne enote itd. Podrobneje so tipi lokacij opisani v poglavju "Vrste nadomestnih lokacij". Vsak tip lokacije ima svoje prednosti in svoje slabosti. Organizacija lahko izbere primeren tip rezervne lokacije glede na svojo odvisnost od informacijskega sistema ter glede na določitev najdaljše dovoljene prekinitve delovanja informacijskega sistema.

Periodično preizkušanje načrta okrevanja po nesrečah

Načrt okrevanja po nesrečah hitro zastara, če se ga ne preizkuša redno. Zato ga je treba neprestano preizkušati z različnimi preizkusi, da se zagotovi in preveri, ali je načrt delujoč in popoln. Spremembe v osebju, opisih delovnih mest, tehnologiji, ureditvi poslovnih prostorov ter socialnega in ekonomskega okolja lahko zahtevajo spremembo postopkov in navodil v načrtu okrevanja po nesrečah.

Vzdrževanje načrta okrevanja po nesrečah
Učinkovit načrt okrevanja po nesrečah mora biti neprestano vzdrževan. Načrt postane zastarel, takoj ko se v informacijski sistem vključi nova aplikacija ali pa se spremeni poslovna politika organizacije. Zaradi tega mora biti načrt posodobljen takoj, ko se zgodijo spremembe v informacijskem sistemu oz. druge relevantne spremembe. Načrt okrevanja po nesrečah mora biti čim pogosteje revidiran. Ob uporabi zastarelega načrta okrevanja po nesrečah se lahko zgodi, da organizacija ne bo mogla obnoviti svojega poslovanja v primeru nesreče.

Zavarovalno kritje za škodo v informacijskem sistemu
Zavarovanje samo po sebi z ničemer ne vpliva na verjetnost dogodka nesreče, vendar v primeru nesreče pomaga poravnati nekatere vrste stroškov ter s tem zmanjša finančni vpliv obnovitve informacijskega sistema na delovanje organizacije. V primeru nesreče lahko nastane tudi problem zmožnosti plačila zapadlih dolgov organizacije. V primeru, da ima organizacija ustrezno zavarovalno polico, tega problema ni.

2.7 Vloge posameznih oddelkov

Izdelava načrta okrevanja po nesrečah ni naloga posameznika. Potrebno je strokovno znanje, iznajdljivost in sodelovanje zaposlenih na vseh ravneh odločanja. Dobro pripravljen načrt okrevanja po nesrečah zahteva sodelovanje vodilnih delavcev, oddelka informacijske tehnologije ter kadrovnikov. Vsi skupaj se morajo pripraviti in sodelovati pri ozaveščanju zaposlenih in pri nalogah, kot so: zagotavljanje računalniške varnosti, varovanje podatkov itd. V nadaljevanju je prestavljena udeležba in naloge zgoraj naštetih oddelkov, ki so povzete po Hawkins, Yen, Chou (2000, str. 225).

2.7.1 Udeležba in naloge vodilnih delavcev

Biti seznanjen z informacijsko tehnologijo
Vodilni delavci večinoma nočejo biti soočeni z informacijsko tehnologijo. Obstajajo trije glavni razlogi za to. Kot prvo "se nimajo za računalnikarje" in posledično prepustijo upravljanje informacijske tehnologije svojim podrejenim ali zaposlenim na oddelku informacijske tehnologije. Kot drugo, bi se mogoče radi izobrazili na področju informacijske tehnologije, vendar so zasuti in zmedeni z oblico literature, ki je na voljo. Lahko pa so tudi prestrašeni ter se čutijo ogrožene s strani kolegov z oddelka informacijske tehnologije, ki se spoznajo na nekaj, na kar se oni ne. Kot vodilni delavci se lahko počutijo ogrožene zaradi pomanjkanja razumevanja informacijskega področja ter se popolnoma izogibajo informacijskih zadev. Vendar če imajo vodilni delavci zadovoljivo znanje s področja informacijske tehnologije oz. če ga pridobijo z izobraževanjem, jim to pomaga pri sprejemanju boljših odločitev, bolje se zavedajo pomembnosti zaščite podatkov ter lažje komunicirajo z zaposlenimi z oddelka informacijske tehnologije.

Zaposlovanje kvalificiranih strokovnjakov

Posamezniki, ki so imetniki certifikatov, lahko dokažejo svojo vrednost in znanje. Microsoft Computer Systems Engineer (MCSE) for Windows 2000, Certified Novel Engineer (CNE) for Novel Networks in Red Hat Certified Engineer (RHCE) so samo nekateri od primerov certifikatov s področja informacijske tehnologije. Če namerava organizacija izgraditi podatkovno omrežje, se lahko odloči zaposliti strokovnjaka s certifikatom Cisco Certified Network Associate (CCNA) ali pa Cisco Certified Internetwork Engineer (CCIE). Zaposlovanje strokovnjakov s certifikati prihrani organizaciji tudi čas in denar, ki bi ga morala nameniti izobraževanju le-teh.

Podobno kot zgornji certifikati obstajajo tudi certifikati s področja načrtovanja okrevanja po nesrečah. Primer organizacije, ki ponuja izobraževanje in certificiranje s področja načrtovanja okrevanja po nesrečah, je Disaster Recovery Institute[2].

Zagotovitev primernega zavarovalnega kritja

Obsežna zavarovalna polica lahko vključuje povrnitev stroškov obnove podatkov in prekinitve poslovanja, stroškov okrevanja, nadomestitve poškodovane računalniške opreme v primeru naravnih nesreč, kot so poplave, potresi ali orkani. Organizacija mora zagotoviti primerno kritje za vsa geografska področja, na katerih posluje.

Ustanovitev skupin za izvedbo načrta okrevanja po nesrečah

Načrt okrevanja po nesrečah mora biti neprestano aktualen in vsak član skupine, ki sodeluje pri okrevalnem postopku, mora biti dobro seznanjen z njegovo vsebino. Implementacija načrta okrevanja po nesrečah mora vsebovati tudi sestavo posebnih skupin, ki so odgovorne za določeno področje. Primeri takšnih skupin so: prva odzivna skupina, obnovitvena skupina, skupina za obnovitev procesov in skupina za logistično podporo.

Prva odzivna skupina

Ta skupina prva oceni naravo in obseg škode. Člani te skupine se odločijo, če se poslovni procesi lahko nadaljujejo na prizadeti lokaciji ali pa jih je treba preseliti na alternativno lokacijo. Če je škoda velika, bo ta skupina tista, ki bo vzpostavila zvezo z drugimi skupinami ter jih aktivirala.

Obnovitvena skupina

Ta skupina usklajuje restavracijo in ponovno aktivacijo delov informacijskega sistema, kot so: podatkovne datoteke, programska oprema, omrežna infrastruktura, komunikacijski vodi itd.

Skupina za obnovitev procesov

Če člani prve odzivne skupine ugotovijo, da je potrebno poslovne procese preseliti na alternativno lokacijo, potem obnovitvena skupina uredi in zagotovi izvajanje poslovnih procesov na alternativni lokaciji. Ta skupina je med drugim odgovorna za vzpostavitev omrežne infrastrukture do

[2] Spletna stran inštituta: http://www.drii.org.

alternativne lokacije, za pridobitev varnostnih kopij, namestitev strojne opreme in komunikacijskih vodov.

Skupina za logistično podporo
Med prenosom poslovnih procesov na alternativno lokacijo je naloga te skupine logistična podpora. Zagotoviti morajo, da lahko zaposleni dostopajo do poslovnih prostorov na alternativni lokaciji. Nudijo tudi osebno pomoč zaposlenim, kar vključuje pomoč pri potovanjih in selitvah, finančno pomoč za nujne izdatke, krizno svetovanje in pomoč družini zaposlenega.

2.7.2 Udeležba in naloge oddelka informacijske tehnologije

Izdelava natančnega načrta omrežja
Če nesreča uniči del ali celotno zgradbo, kjer je delovala organizacija, potem je nujna ponovna izgradnja omrežja. Načrt arhitekture omrežja organizacije omogoči zaposlenim v oddelku informacijske tehnologije, da ponovna izgradnja omrežja traja čim manj časa.

Zagotovitev podpore vodstva za načrtovanje okrevanja po nesrečah
Ni nujno, da se vodstvo podjetja zaveda nevarnosti izgube podatkov. Naloga vodje informacijskega oddelka je, da ta problem primerno predstavi vodilnim delavcem in pridobi njihovo podporo pri izvajanju procesov, povezanih z načrtovanjem okrevanja po nesrečah.

Nadziranje dostopa do interneta
Medtem ko internet omogoča hiter dostop do informacij po celem svetu, predstavlja internet tudi veliko varnostno grožnjo. Že v sami zasnovi interneta je premalo varnostnih mehanizmov, saj je težko ugotoviti, od kod podatki prihajajo oz. kam gredo. Za organizacije je zato priporočljivo, da nadzirajo dostop do interneta s požarnimi zidovi. Tako zmanjšajo tveganje vdora z interneta v svoje omrežje.

Standardizacija strojne in programske opreme
Vsaka organizacija, ki uporablja heterogeno programsko ali strojno opremo, bo imela težave pri ponovni izgradnji svojega omrežja. Če na primer nekateri oddelki uporabljajo Macintosh računalnike, drugi pa osebne računalnike, bo obnova informacijskega sistema izredno težka. Zato je priporočljivo imeti homogeno programsko in strojno opremo, saj to zmanjša kompleksnost ponovne izgradnje omrežja.

Zagotovitev podpore dobaviteljev
Implementacija načrta okrevanja po nesrečah mora zagotoviti podporo rutinskih dobaviteljev in specializiranih dobaviteljev. Rutinski dobavitelji so podjetja, katerih storitve uporabljajo organizacije dnevno (strojna podpora, programska podpora, podpora elektronskega poslovanja, telekomunikacijske storitve). Specializirani dobavitelji so podjetja, ki zagotavljajo določene storitve

okrevanja po nesrečah. Njihove storitve vključujejo reševanje podatkov, obnovo podatkov, alternativne pisarniške prostore, alternativne prostore, namenjene varnostnim kopijam, in nujen najem strojne opreme in pisarniške opreme.

Izdelava varnostnih kopij

Postopek izdelovanja varnostnih kopij mora zagotoviti, da se vsi potrebni podatki prenašajo na strežnik za izdelavo varnostnih kopij ter da se ne nahajajo na medijih, ki niso vključeni v izdelavo varnostnih kopij (disketne enote, CD enote, ZIP enote, USB pomnilniški mediji ipd.). To zagotavlja, da se varnostne kopije nahajajo na eni lokaciji[3], kar zagotavlja učinkovito upravljanje varnostnih kopij, ter obnovo podatkov iz njih.

Zagotovitev povezav med osrednjimi računalniki ter strežniki in odjemalci

Poiskati in določiti je treba vse vmesniške aplikacije, ki služijo za povezavo osrednjih računalnikov z drugimi deli omrežja. Te aplikacije morajo biti nato vključene v proces izdelave varnostnih kopij in v okrevalne načrte. Če organizacija nima na razpolago dobrih varnostnih kopij teh aplikacij, ima lahko velike probleme pri okrevanju svojega informacijskega sistema in pri integriteti podatkov in sistema.

Uporaba tehnologije skupine neodvisnih diskov s preobiljem podatkov za tekoče transakcije

Tehnologija skupine neodvisnih diskov s preobiljem podatkov zagotavlja zrcaljenje podatkov na več diskov, na katerih so zmeraj zadnje verzije datotek. S to tehnologijo se tudi zavarujemo pred strojnimi napakami, če se le te zgodijo na delu diskovja. V primeru odpovedi enega diska so podatki še vedno na voljo na drugih diskih.

Zaščita pred računalniškimi virusi

Uporaba proti-virusnih programov je nujna za zavarovanje informacijskega sistema pred virusi. Sistemski administratorji morajo delati redne preglede medijev s proti-virusnimi programi, prav tako pa morajo biti vključeni pregledovalniki virusov v realnem času.

Zaščita strojne opreme pred škodo iz okolja

Strežniki morajo biti zavarovani pred previsokim napetostmi električnega toka in pred vplivi statične elektrike. Prav tako mora biti strojna oprema zaščitena pred drugimi nevarnostmi, kot so npr. razlitje vode, požar, fizične poškodbe itd.

Zagotovitev sistema neprekinjenega napajanja

Prekinitve pri dobavljanju električne energije so en od glavnih vzrokov izgube podatkov. Če se strežniku nenadoma prekine dovajanje električne energije, je velika verjetnost, da bomo izgubili del podatkov na njem. Z namestitvijo sistemov neprekinjenega napajanja in/ali varnostnega električnega generatorja zagotovimo delovanje strežnikov, ki so priključeni na ta sistem, tudi ob prekinitvi

[3] Sistemi za varnostne kopije imajo po navadi kopije podatkov zapisane na več medijih, ki so geografsko ločeni. Vendar predstavlja vse skupaj en sistem za izdelavo varnostnih kopij.

dobave električne energije iz primarnega vira. Tako se zavarujemo pred izgubo podatkov zaradi prekinitve dobave električne energije. Večinoma se na sistem neprekinjenega napajanja priključi samo ključne strežnike.

2.7.3 Udeležba in naloge kadrovskega oddelka

Izvajanje izobraževanja o pravilni uporabi računalnikov in o računalniški etiki
Zaposleni lahko prenese virus s svojega domačega računalnika na računalnik v organizaciji ter tako poškoduje računalniško informacijski sistem organizacije. Naloga kadrovskega oddelka je informirati in izobraziti zaposlene o nevarnostih računalniških virusov ter zagotoviti, da zaposleni ne prinašajo v organizacijo osebnih podatkov (ki bi lahko vsebovali viruse).

Nesreče se lahko zgodijo tudi zaradi neetičnega ravnanja uporabnikov računalnikov. Etično ravnanje uporabnikov računalnikov postaja predmet razprave v organizacijah. V dobi, v kateri so postali računalniki bistven del družbe ter se uporabljajo na vseh področjih življenja, so mnoge organizacije odkrile, da lahko zaposleni, ki uporabljajo računalnike nepravilno, povzročijo organizaciji veliko izgubo v informacijah, času in tudi denarju. Zato mnoge organizacije uvajajo pravilnike o uporabi računalnika kot sestavni del pogodbe o zaposlitvi.

Izobraževanje o varnosti v primeru nesreč
Načrt okrevanja po nesrečah lahko vsebuje mnogo scenarijev – od pokvarjenega omrežja do popolnega uničenja poslovne zgradbe. Vodstveni delavci morajo ob upoštevanju geografske lokacije v načrt okrevanja po nesrečah vključiti izobraževanje o varnosti v primeru nesreč. S tem zagotovijo pripravljenost in izurjenost zaposlenih za primer naravnih nesreč kot npr. potresa, orkana, poplave. Program lahko vključuje izobraževanje o prvi pomoči, urjenje za primer požara ter določitev varnih območij v primeru nesreče.

2.8 Razvoj načrta okrevanja po nesrečah

Vsaka organizacija, ki začenja z izdelavo načrta okrevanja po nesrečah, mora najprej narediti oceno tveganosti informacijskega sistema. To vključuje pregled njihovih sistemskih sredstev in določitev virov, ki so nujno potrebni za dnevno opravljanje poslovnih operacij. Po opravljeni analizi je treba pripraviti načrt aktivnosti. Le-ta je lahko kratek seznam opravil ali pa so to navodila za uporabo v več zvezkih. Po izdelavi lahko organizacija ta načrt vključi v njene poslovne procese. Organizacija mora poskrbeti tudi za izobraževanje zaposlenih ter jasno definirati naloge vsakega zaposlenega v zvezi z načrtom okrevanja po nesrečah. Proces izdelave načrta bi moral biti obnovljen vsaj enkrat letno. Ob tem se dodajo spremembe, ki so bile spregledane, zaposleni pa obnovijo svoje znanje.

Načrtovanje okrevanja po nesrečah sestoji iz definiranja pravil in postopkov, tako da se zagotovi delovanje kritičnih poslovnih procesov, četudi odpove en ali več elementov informacijskega

sistema, od katerih so ti poslovni procesi odvisni. Ključne faze pri razvoju načrtovanja okrevanja po nesrečah so:

- ustanovitev projektne skupine,
- izdelava analize tveganja,
- določitev prioritet za aplikacije in omrežja,
- izdelava okrevalnih strategij,
- izdelava inventarja in dokumentacije načrta,
- določitev overovitvenih kriterijev in postopkov,
- implementacija načrta.

Ključne osebe iz vsakega oddelka bi morali biti člani projektne skupine. Sodelovati bi morali pri vseh načrtovalnih procesih izdelave načrta okrevanja po nesrečah. Projektna skupina se mora spoznati na poslovne procese, tehnologijo, omrežja in sisteme, da lahko uspešno izdela načrt okrevanja po nesrečah.

Projektna skupina mora narediti oceno tveganja in analizo vpliva na poslovne procese vsaj za najpomembnejših deset nesreč. Po analizi tveganja je treba vsakemu poslovnemu procesu in aplikaciji (sistemu) določiti stopnjo prioritete. Pomembno je, da se inventar nenehno obnavlja ter da ima organizacija vedno na voljo najnovejše podatke o opremi, lokacijah, dobaviteljih in kontaktnih osebah.

Cilj je, da se napravi delujoč, efektiven, ter stroškovno učinkovit načrt za okrevanja vseh delov informacijskega sistema. V tabeli 3 je prikazan en od možnih načinov razvrstitve delov informacijskega sistema. S pomočjo razvrstitve delov informacijskega sistema glede na izpostavljenost in kritičnost se določi, kakšna stopnja obnovitve je potrebna.

Tabela 3: Razvrstitev delov informacijskega sistema glede na izpostavljenost in kritičnost[4]

Razvrstitev	**Opis**
Kritično za poslanstvo	Kritično za dosego poslanstva organizacije. Lahko je opravljeno samo z računalniki. Alternativni ročni postopek ne obstaja. Mora biti obnovljeno v 36 urah.
Kritično	Kritično za dosego delovnih nalog organizacije. Večinoma je opravljeno z računalniki. Ročni postopek je možno izvajati samo za krajše časovno obdobje. Mora biti obnovljeno v petih dneh.
Bistveno	Bistveno za dosego delovnih nalog organizacije. Opravljeno z računalniki. Ročni postopek je možno izvajati za daljše časovno obdobje. Naj bi bilo obnovljeno v petih dneh, vendar je lahko ta čas daljši.
Nekritično	Nekritično za dosego poslanstva organizacije. Obnovitev se lahko odloži, dokler ni obnovljen informacijski sistem oz. dokler ni dobavljena nova računalniška oprema. Lahko je opravljeno ročno.

Vir: Bahan, 2003, str. 3.

V literaturi najdemo tudi drugačne pristope določitve, katere dele informacijskega sistema je treba vključiti v načrt okrevanja po nesrečah. Lee in Ross (1995, str. 21) predlagata matriko (tabela 4), ki lahko služi pri odločanju, katere dele informacijskega sistema se bo vključilo v načrt okrevanja po nesrečah in katere ne. S pomočjo spodnje matrike je možno določiti tudi prioritete, kateri deli sistema bodo vključeni prej ter kateri kasneje.

Tabela 4: Določitev prioritet vključevanja delov informacijskega sistema v načrt okrevanja po nesrečah

Kritičnost / **Ranljivost**	*Visoka*	*Nizka*
Velika	zagotovo	manj verjetno
Majhna	verjetno	malo verjetno

Vir: Lee, Ross, 1995, str. 21.

Namen načrta okrevanja po nesrečah je ponovna obnovitev delovanja sistemov, ki podpirajo kritične poslovne procese in poslovne procese, ki so kritični za poslanstvo. Cilj organizacije je, da se vzpostavi normalno stanje v najmanjšem možnem času. Ker so mnogi poslovni procesi kritični in kritični za poslanstvo, odvisni od tehnične infrastrukture, ki sestoji iz aplikacij, podatkov in strojne opreme, mora biti načrt okrevanja po nesrečah osredotočen na informacijski sistem. Organizacija mora izdelati načrt okrevanja po nesrečah za vse svoje aplikacije. Obnovitev sistema ne zahteva nujno podvojevanja strojne in programske opreme. V načrtu okrevanja po nesrečah so lahko navedeni postopki, ki so v celoti ročni. Odločitev, ali uporabiti ročni postopek ali pa se odločiti za popolnoma avtomatiziran postopek, je ponavadi odvisna od razpoložljivih finančnih sredstev.

[4] Navedeni časi obnove so samo primeri, saj so odvisni od značilnosti poslonih procesov organizacije.

Prisotnost delujočega načrta okrevanja po nesrečah zmanjša verjetnost, da bo čas okrevanja daljši od časa, ki je bil določen s strani vodstva organizacije za posamezne dele informacijskega sistema. Med fazo obnavljanja sistema pa je poudarek na zagotovitvi nadzora nad tekočimi dogodki, da se prepreči dodatne izgube podatkov (ali drugih virov).

Izdelava tehničnega dela načrta okrevanja po nesrečah je samo en del izdelave celotnega načrta. Proces izdelave tehničnega dela načrta je skupen vsem informacijskim sistemom ter poteka v naslednjih korakih:

1. izdelava politike načrta neprekinjenega poslovanja in prioritet poslovnih procesov,
2. izdelava analize tveganja,
3. izdelava analize vpliva na poslovanje,
4. izdelava strategij neprekinjenega poslovanja in strategij okrevanja,
5. izdelava načrtov neprekinjenega poslovanja,
6. seznanitev, testiranje in izobraževanje v zvezi z načrtom okrevanja po nesrečah,
7. vzdrževanje načrta okrevanja po nesrečah ter izvajanje vaj.

Namen izdelave analize vpliva na poslovanje je določitev ciljev za obnovitev računalniških sistemov, na katerih se izvajajo aplikacije, ki podpirajo izvajanje poslovnih procesov. Cilji so določeni kot kritični obnovitveni čas in kritična obnovitvena točka. Kritični obnovitveni čas je število ur ali dni, v katerih mora biti sistem obnovljen. Kritična obnovitvena točka določa največjo starost podatkov, ki jih je možno obnoviti v primeru nesreče. Na primer, če je kritična obnovitvena točka osem ur, potem mora biti organizacija sposobna obnoviti podatke do trenutka, ki ni starejši od osmih ur pred nesrečo. Pri izbiri strategije načrta okrevanja po nesrečah sta najpomembnejša dejavnika kritični obnovitveni čas in kritična obnovitvena točka. Ta dva dejavnika namreč v največji meri vplivata, kakšna strategija načrta okrevanja po nesrečah bo izbrana za določen sistem oz. del sistema.

Kritični obnovitveni čas in kritična obnovitvena točka sta dva cilja, ki ju mora vodstvo upoštevati pri določanju pogojev za neprekinjeno poslovanje podjetja. Kritičen obnovitveni čas upošteva vodstvo podjetja kot potreben čas, da se obnovijo deli informacijskega sistema, da lahko posledično kritične aplikacije delujejo. Vendar pa vodstvo podjetja rado pozabi na kritično obnovitveno točko. Medtem ko se zgodi nesreča, podjetje izgubi podatke; ravno to pa je vprašanje, na katero je treba odgovoriti: koliko podatkov lahko podjetje izgubi ter kako sodobni bodo obnovljeni podatki. Banka, na primer, si ne more privoščiti, da bi izgubila podatke za šest ur nazaj, medtem ko si lahko organizacija v kakšni drugi panogi to lahko privošči. Vodstvo podjetja se mora odločiti, katere stopnje tveganja so še sprejemljive.

Določitev aplikacij

Za poslovne procese, katerim je vodstvo podjetja določilo kritične obnovitvene čase in kritične obnovitvene točke, je treba določiti, katere aplikacije jih podpirajo ter katere podatke uporabljajo. Kot smo že prej navedli, so aplikacije razvrščene glede na kritičnost kot: kritične za poslanstvo,

kritične, bistvene ali nekritične. V večini primerov je en poslovni proces odvisen od več aplikacij. Aplikacijam se dodelijo enaki kritični obnovitveni časi in kritične obnovitvene točke, kot so bili dodeljeni poslovnim procesom, ki jih podpirajo. Če neka aplikacija podpira poslovne procese z različnimi kritičnimi obnovitvenimi časi/točkami, se ji dodeli najnižjo od vseh vrednosti kritičnega obnovitvenega časa/točke.

Določitev časa okrevanja sistema

Aktivnosti okrevanja sistema se pričnejo, ko je nesreča potrjena. Organizacija mora načrtovati vrstni red prioritet, ki jih bo uporabila v primeru nesreče, za določitev vrstnega reda okrevanja strojne opreme in njenih komponent. Prioritete morajo biti določene tako, da bo organizacija dosegla zastavljene kritične obnovitvene čase za posamezne poslovne procese. Dostikrat se namreč zgodi, da se v načrtu okrevanja po nesrečah v kratkih rokih obnovitvenih časov pozabi na okrevanje sistemov, ki gostujejo aplikacije. Te aplikacije pa so potrebne za izvajanje poslovnih procesov. Določiti je treba, katera strojna oprema in njene komponente podpirajo izvajanje katerih aplikacij, na kateri strojni opremi so shranjeni kateri podatki, ki podpirajo izvajanje poslovnih procesov. Določiti je treba tudi vse medsebojne odvisnosti med aplikacijami, komponente omrežne infrastrukture ter osebje, ki upravlja te aplikacije in strojno opremo. Kritični obnovitveni čas se uporablja za določitev časa okrevanja sistema posameznih komponent strojne opreme ter sega od poslovnih procesov do aplikacij.

Če čas okrevanja sistema določenih komponent strojne opreme ne ustreza pričakovanjem, ki so določeni za poslovne procese, se lahko le-ta na več načinov popravi. Določi se lahko drugačen način okrevanja, ki ugodi zahtevam obnovitvenih časov poslovnih procesov. Lahko se tudi zmanjša čas za prijavo alarma, čas za ocenitev alarma ter čas za objavo nesreče. Na podlagi stroškovne analize, se lahko ponovno določi tu že določene kritične obnovitvene čase poslovnih procesov. Ker lahko strojna oprema gosti več aplikacij, ki se uporablja za več poslovnih procesov z različnimi kritičnimi obnovitvenimi časi, se čas okrevanja sistema določi za aplikacijo z najkrajšim kritičnim obnovitvenim časom, ki je odvisen od strojne opreme.

Sistem, na katerem se izvajajo aplikacije (računalniški sistem), sestoji iz vseh komponent strojne opreme. To vključuje procesno enoto računalniškega sistema, aplikacije, podatkovne sisteme in podatkovne medije, podatkovna omrežja ter varnostno infrastrukturo (npr. požarni zid). Komponente, ki je jih treba določiti za uspešno določitev časa okrevanja sistema, so:

- določitev poslovnih procesov,
- določitev zahtev kritičnega obnovitvenega časa,
- določitev zahtev kritične obnovitvene točke,
- določitev aplikacijskih sistemov, ki podpirajo poslovne procese,
- določitev računalniških sistemov, ki podpirajo aplikacije,
- določitev obnovitvenih časov za računalniške sisteme in aplikacije.

Določitev toka podatkov za aplikacije

Za zagotovitev kritičnih obnovitvenih časov aplikacij je treba izvajati določene aktivnosti že pred nastopom nesreče. Ko se zgodi nesreča, so aplikacije in podatki na prizadeti lokaciji neuporabni za potrebe okrevanja. Zaradi tega mora informacijski sistem med normalnim delovanjem poskrbeti za kopiranje podatkov in aplikacij na oddaljeno lokacijo. Oddaljena lokacija je lahko lokacija, kjer je nameščen rezervni (okrevalni) računalniški center, ali pa oddaljena lokacija, ki je namenjena samo hranjenju podatkov. V drugem primeru morajo biti transportne poti med lokacijo, kjer se hranijo podatki, ter lokacijo, kjer se bo informacijski sistem obnovil, takšne, da prevoz medijev s podatki iz ene lokacije na drugo ne bo ogrozil dosege kritičnega obnovitvenega časa aplikacij, ki se obnavlja. Obstajata dva načina prenosa podatkov s produkcijske lokacije na oddaljeno lokacijo:

- elektronsko kopiranje podatkov in aplikacij iz produkcijske lokacije na oddaljeno lokacijo preko podatkovnega omrežja. Pri prvem kopiranju se na oddaljeno lokacijo prenesejo vse aplikacije in podatki, medtem ko se pri naslednjih kopiranjih prenesejo samo spremenjeni podatki (datoteke itd.) in spremenjene aplikacije.
- Kopiranje podatkov na medij, ki ga je možno fizično ločiti od naprave, v kateri je bil zapisan, ter ga prenesti na oddaljeno lokacijo. Najpogosteje uporabljen medij so tračne enote.

Kopije aplikacij in podatkov morajo zapustiti produkcijsko lokacijo v časovnem okviru, ki ne sme biti večji od kritične obnovitvene točke, saj se le tako lahko zagotovi obnovitev podatkov, ki ustreza zahtevam, določenim z kritično obnovitveno točko. To še posebej velja za podatke, ki se fizično prenašajo na medijih (npr. tračnih enotah). Varnostna kopija podatkov in aplikacij mora biti narejena ter prenesena iz produkcijske lokacije v časovnem okviru kritične obnovitvene točke.

Določitev kritičnega osebja in obnovitvenih skupin

Aplikacije in sistemi, ki podpirajo kritične poslovne procese, so odvisni od osebja s posebnimi znanji in sposobnostmi. Določitev osebja, ki zna in je zmožno obnoviti infrastrukturo, za podporo poslovnih procesov, je en izmed ključnih delov načrtovanja okrevanja po nesrečah. Bistveno osebje mora biti določeno skupaj z njihovim strokovnim znanjem. Znanje, ki ga je potrebno uporabiti pri okrevanju v primeru nesreče, mora biti geografsko razpršeno po organizaciji, saj se tako zagotovi, da ima organizacija dovolj primernega osebja za potrebe okrevanja po nesreči, če se nesreča zgodi. Strokovna znanja in sposobnosti zaposlenih morajo biti tudi dokumentirana v načrtu okrevanja po nesrečah ter posodobljena z enako pogostostjo kot sam načrt okrevanja po nesrečah.

Določitev možnih ranljivosti

Nadzorovanje ranljivosti v večini primerov prepreči probleme, preden le ti nastanejo. V večini organizacij lahko nastanejo problemi, povezani z ranljivostjo, na naslednjih področjih (Hawkins, Yen, Chou, 2000, str. 227):

- lokacije hranjenja varnostnih kopij,
- računalniška varnost,
- fizično varovanje,
- prostor oz. zgradba, v kateri se nahajajo računalniki,

- električni tok,
- javljanje požara in gašenje požara,
- odvisnost od ene osebe za informacije,
- nadzor s strani vodilnih delavcev,
- zanesljivost telekomunikacijskih storitev.

Druga področja, povezana z ranljivostjo so še: odpoved delovnega razmerja s strani delavcev, virusi itd.

Preizkušanje načrta okrevanja po nesrečah

Da bi bili preizkusi načrta okrevanja po nesrečah čim bolj učinkoviti, je treba določiti cilje preizkusov ter objektivne preizkusne kriterije. S pomočjo ciljev preizkusov in z objektivnimi preizkusnimi kriteriji se omogoči ocenitev učinkovitosti posameznih delov načrta okrevanja po nesrečah in tudi celotnega načrta neprekinjenega delovanja. Glavna preizkusna kriterija sta obnovitev poslovnih procesov v času kritičnega obnovitvenega časa ter zagotovitev veljavnih podatkov v času, določenem s kritično obnovitveno točko:

- kritični obnovitveni čas
    - Časovni okvirji za prijavo alarma, ocenitev alarma ter objavo nesreče so preizkušeni ter potrjeni. Standardni postopki so preizkušeni ter potrjeni, da so pravilni. Prav tako so potrjeni vsi podatki o kontaktnih osebah.
    - Čas okrevanja sistema je upoštevan pri kritičnih obnovitvenih časih aplikacij. Čas okrevanja sistema je preizkušen na primeru okrevanja sistema ter je potrjeno, da se lahko doseže zastavljene čase okrevanja sistema.
- Kritična obnovitvena točka je potrjena ter jo je mogoče doseči. Preverjeni so standardni postopki izdelave varnostnih kopij ter prenosa podatkov varnostnih kopij na oddaljeno lokacijo ter posledično je potrjeno, da je mogoče doseči zastavljene kritične obnovitvene točke.

Preizkušanje načrta okrevanja po nesrečah je lahko zelo kompleksna naloga. Več o načinih preizkušanja načrta okrevanja po nesrečah je napisano v poglavju "Preizkušanje načrta okrevanja po nesrečah".

Glavni namen načrta neprekinjenega poslovanja je zagotoviti nadaljevanje izvajanja poslovnih procesov, medtem ko je glavni namen načrtovanja okrevanja po nesrečah repliciranje delov ali celotnega informacijskega sistema na alternativno lokacijo, dokler se stanje ne normalizira ter se zopet vzpostavi prejšnje stanje.

Vzdrževanje načrta okrevanja po nesrečah

Vzdrževanje načrta okrevanja po nesrečah ter drugih delov načrta neprekinjenega poslovanja je ključno za uspešno okrevanje v primeru nesreče. Načrti morajo odražati spremembe, ki se zgodijo v informacijskem sistemu in poslovnih procesih, ki informacijski sistem podpira, ter morajo biti neprestano obnavljani.

2.8.1 Življenjski cikel načrta okrevanja po nesrečah

Celoten postopek izdelave načrta okrevanja po nesrečah lahko povzamemo v treh stopnjah: načrtovanje, prevzem, ovrednotenje (Hawkins, Yen, Chou, 2000, str. 224).

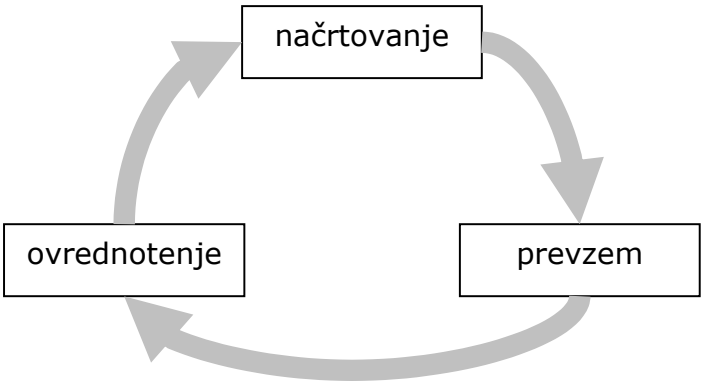
Razvoj načrta okrevanja po nesrečah se začne s procesom načrtovanja. Med procesom načrtovanja, se ideje in koncepte pretvori v jasne naloge in postopke. Ustanovi se odbor za planiranje, ki vključuje predstavnike oddelkov organizacije. Odbor izvede analizo tveganja za vsak oddelek v organizaciji ter tako določi posledice nesreče ter potencialno škodo, ki jo nesreča lahko povzroči. Po končani analizi se naredi načrt aktivnosti, ki se predstavi vodilnim delavcem.

Po odobritvi načrta aktivnosti s strani vodilnih delavcev se načrt okrevanja po nesrečah sprejme in integrira v dnevno delovanje organizacije. To je proces prevzema, ki vključuje med drugim tudi: izobraževanje zaposlenih, ozaveščanje zaposlenih, spreminjanje opisa delovnih nalog in integriranje načrta okrevanja po nesrečah v vsakodnevno delovanje organizacije.

Sledi proces nenehnega ovrednotenja načrta okrevanja po nesrečah. Vodilni delavci morajo redno (npr. vsake pol leta) in po potrebi (npr. ob namestitvi nove strojne opreme) pregledovati in ponovno ovrednotiti načrt okrevanja po nesrečah. Če se je stanje v organizaciji spremenilo, je treba načrt okrevanja po nesrečah spremeniti (proces načrtovanja) ter spremembe v načrtu okrevanja po nesrečah tudi integrirati v delovanje organizacije (proces prevzema).

Vidimo, da je izdelava (in vzdrževanje) načrta okrevanja po nesrečah proces, ki se nikoli ne konča. Celoten proces lahko grafično predstavimo z diagramom procesa (slika 1).

Slika 1: Življenjski cikel izdelave načrta okrevanja po nesrečah



Vir: Hawkins, Yen, Chou, 2000, str. 224.

2.9 Preizkušanje načrta okrevanja po nesrečah

Organizacije morajo redno obnavljati načrt okrevanja po nesrečah. Z rastjo in spreminjanjem organizacije rastejo in se spreminjajo tudi njeni podatki, procesi, oprema itd. Če organizacija ne obnavlja svojega načrta okrevanja po nesrečah, se lahko zgodi, da v primeru nesreče ne bo mogla obnoviti svojega informacijskega sistema in svojih procesov. Hitro rastoče in hitro spreminjajoče se organizacije pa morajo obnavljati svoje načrte okrevanja po nesrečah še intenzivneje kot druge organizacije.

Mnoga podjetja izdelajo dober načrt okrevanja po nesrečah, ki pa ga nikoli ne obnavljajo. Imeti takšen načrt okrevanja po nesrečah je lahko slabše, kot pa če ga podjetje sploh ne bi imelo, saj daje zaposlenim lažen občutek varnosti.

Dva glavna razloga, zakaj podjetja ne preizkusijo svojih načrtov okrevanja po nesrečah, sta: "preveliko zaupanje v informacijski oddelek" in "predragi in težko izvedljivi preizkusi." (Edwards, Cooper, 1995, str. 21). V primeru nesreče zaposleni delajo nadpovprečno, vendar tudi če vložijo veliko truda, ne morejo obnoviti varnostnih kopij, ki se niso izdelale, ker načrt okrevanja po nesrečah ni bil preizkušen. Po drugi strani pa ni treba vedno preizkusiti celotnega načrta okrevanja po nesrečah, saj se lahko z delnimi preizkusi preveri celoten načrt okrevanja po nesrečah z nizkimi stroški.

2.9.1 Tipi preizkusov

Pred izvedbo revizije načrta okrevanja po nesrečah je potrebno določiti programe preizkusov. Na voljo so štirje tipi preizkusov, ki jih lahko podjetje uporabi:

- hipotetični preizkus (preizkus, ki ne vsebuje praktičnih testov),
- komponentni preizkus (preverjanje natančnosti in natančnosti posameznih postopkov),
- modularni preizkus (preizkus, ki ga lahko kombiniramo z drugimi moduli) ter
- poln preizkus (potrebujemo za preizkusu namenjeno strojno opremo).

Glede na kompleksnost svojega informacijskega sistema se podjetje odloči, ali bo izvedlo vse preizkuse ali pa bo preskočilo katero od stopenj. Podjetja s preprostimi informacijskimi sistemi lahko izvedejo takoj poln preizkus, medtem ko morajo podjetja s kompleksnejšimi informacijskimi sistemi pričeti pri hipotetičnem preizkusu. Pri vseh preizkusih, razen hipotetičnem, se tudi meri čas, potreben za izvedbo preizkusa. Tako lahko kasneje ocenimo, koliko časa bi dejansko okrevanje trajalo, ter vidimo, ali se nahajamo znotraj časovnih okvirov, določenih v načrtu okrevanja po nesrečah.

Hipotetični preizkus

Hipotetični preizkus je teoretičen preizkus, pri katerem se ne uporablja nobene strojne ali programske opreme. Uporablja se ga, za preverjanje, ali obstajajo vsi potrebni postopki in naloge, ki so navedeni v načrtu okrevanja po nesrečah, ter da se preveri teoretično delovanje teh postopkov. Takšen preizkus naj bi se izvedel vsakih šest mesecev. Izvedba preizkusa ne zahteva veliko časa. Uporablja se način najslabšega scenarija za strojno opremo, saj se tako zagotovi pregled vseh procesov.

Komponentni preizkus

Komponenta je najmanjši skupek navodil v načrtu okrevanja po nesrečah, ki omogoča izvedbo določenih procesov. Na primer: proces "namestitev operacijskega sistema" vključuje zaporedje ukazov, s katerimi se namesti operacijski sistem. Vendar so lahko zahteve v primeru okrevanja drugačne kot pri normalnem delovanju sistema. V primeru okrevanja je treba nekatere nastavitve določiti drugače, saj je okolje v primeru okrevanja lahko drugačno kot pri normalnem delovanju. Če se ne preizkusi vseh komponent, je možnost nedelovanja sistema pri okrevanju zaradi nezdružljivosti velika. Testiranje komponent je namenjeno preverjanju podrobnosti in natančnosti posameznih postopkov v načrtu okrevanja po nesrečah.

Primeri komponentnih preizkusov:

- namestitev operacijskega sistema,
- postopek izdelave varnostnih kopij,
- shranjevanje medijev varnostnih kopij na oddaljeni lokaciji,
- zaporedje pri okrevanju aplikacij,
- okrevalni postopki,
- pregled nadomestne lokacije,
- namestitev varnostnih paketov.

Modularni preizkus

Modul je kombinacija komponent. Idealno bi bilo, če bi lahko vsako komponento posebej preizkusili, preden bi jo vključili v modul. Nekatere od komponent se uporablja pri vsakodnevnem delu ter se jih ob tem tudi preizkusi. Namen modularnega testiranja je preizkusiti pravilnost in delovanje okrevalnih postopkov, če se kombinira več komponent skupaj. Če lahko organizacija preveri pravilnost delovanja vseh modulov, pa čeprav ni opravila polnega preizkusa, je lahko vodstvo podjetja prepričano, da bodo v primeru nesreče uspešno obnovili informacijski sistem.

Primeri modularnih preizkusov:

- aktivacija sekundarne lokacije,
- okrevanje omrežja,
- okrevanje baz podatkov,
- okrevanje operacijskega sistema,
- okrevanje aplikacij,
- zagon proizvodnih linij.

Polni preizkus
Polni preizkusu preveri, ali je vsaka komponenta v vsakem modulu delujoča ter da ustreza strategiji in časovnemu okvirju, določenima v načrtu okrevanja po nesrečah. Preizkus preveri tudi medsebojne odvisnosti modulov. Tako se zagotovi prehod iz modula na modul brez težav ali izgub podatkov. Dva glavna cilja polnega preizkus sta:

- potrditev predvidenega časovnega okvirja, potrebnega za okrevanje celotnega sistema, določenega v načrtu okrevanja po nesrečah,
- potrditev učinkovitosti načrta okrevanja po nesrečah, ki zagotavlja tekoč prehod iz modula na modul.

Za dosego prvega cilja potrebuje organizacija v tesnem okolju strojno in programsko opremo podobne zmogljivosti, kakor jo uporablja v danem trenutku. Z dosego drugega cilja ta pogoj ni potreben.

2.9.2 Postavljanje ciljev

Vsak od preizkusov temelji na najslabšem scenariju za opremo. S tem se zagotovi, da se preverijo celoten načrt okrevanja po nesrečah ter vse možne situacije. Osnovni preizkusi, ki temeljijo na najboljšem scenariju za osebje, temeljijo na predpostavki, da so vsi udeleženci prisotni ter da je na voljo vse znanje, potrebno za razumevanje in razreševanje problemov, ki nastanejo med izdelavo načrta. Vse pomanjkljivosti načrtov in možnosti za popravke se morajo zabeležiti ter posredovati odgovornim osebam. Ko je načrt okrevanja po nesrečah pregledan ter je potrjena njegova pravilnost, se lahko preveri drugačne scenarije (npr. najslabši scenarij za osebje). Tako se zagotovi, da so postopki popolni ter da jih lahko izvedejo tudi tehnično manj izkušene osebe. Ko so vse zahteve, ki so povezane s katero od komponent, dokumentirane in preverjene, samo tedaj lahko označimo načrt okrevanja po nesrečah kot popoln in delujoč.

Preden se izvede preizkus, je treba preveriti vse vidike le-tega. Za preizkus je treba predvideti tudi predpostavke, ki pri pravi nesreči mogoče ne bi bile resnične. Naštetih je nekaj primerov:

- izvedba preizkusa lahko potrebuje dogovor z drugimi oddelki, da se prepreči kakršenkoli vpliv na tekoče procese,
- treba je ustaviti nadzor sprememb za čas izvajanja preizkusa,
- treba je preveriti, če se med časom izvajanja preizkusa ne bodo dogajale kakšne druge spremembe v sistemu itd.

Bolje je namreč prestaviti preizkus, kakor aktivirati celotno skupino; ko pa je treba izvesti preizkus, se ugotovi, da je bila neka majhna podrobnost spregledana ter da je treba celoten preizkus preklicati. To pomeni izgubo časa in denarja.

Pri izvajanju preizkusov je treba postaviti cilje. Spodaj so našteti nekateri od teh:

- obnovitev sistemov na oddaljeni lokaciji in vzpostavitev okolja, v katerem bodo izbrane aplikacije delovale izključno na oddaljeni lokaciji,
- pridobitev in predstavitev vse dokumentacije, ki je potrebna za pridobitev in pravilno uporabo varnostnih kopij iz oddaljene lokacije ter za obnovo kritičnih sistemov na izbrani lokaciji,
- uspešna obnovitev operacijskega sistema (ali aplikacije ali baze podatkov ali datotek) iz varnostnih kopij, ki so shranjene na oddaljeni lokaciji,
- pridobitev in predstavitev vse dokumentacije, potrebne za obnovo produkcijskih podatkov na izbrano lokacijo,
- pridobitev in predstavitev vse dokumentacije, potrebne za popolno obnovitev komunikacijskih vodov med izbranimi lokacijami,
- namestitev komunikacijske opreme in vodov, kakor je navedeno v načrtu okrevanja po nesrečah,
- pregled alternativne lokacije ter potrditev, da je vsa oprema, navedena v načrtu okrevanja po nesrečah, dejansko tudi prisotna na alternativni lokaciji.

2.9.3 Določitev mej

Meje preizkusov je treba določiti, da se zadovolji strategiji okrevanja, metodologiji in procesom. Vodilni delavci morajo zagotoviti, da se kriteriji preizkusov spreminjajo v skladu s spremembami v informacijskem sistemu organizacije. Vedno, kadar se pojavi priložnost za izvedbo preizkusa, jo je treba izkoristiti. Te priložnosti se pojavijo največkrat kot nabava nove/dodatne opreme ali kot pogodbe z dobavitelji o uporabi vročih lokacij, hladnih lokacij, ali pogodbe o najemu sistemov na najetih lokacijah. Med izvedbo preizkusov se lahko vključi tudi notranje opazovalce (revizorje, vodstvo), zunanje opazovalce (strokovnjake za varnost podatkov) ali pa kombinacijo obeh.

Scenarij

Scenarij je opis teoretične nesreče. V njem so navedene vse predpostavke, ki so povezane s to nesrečo. Scenarij mora, na primer, vsebovati podatke o tem, kaj je povzročilo nesrečo, kakšna je škoda, povzročena na opremi, ter ali je mogoče kaj rešiti iz ostankov uničene opreme. Namen scenarija ni izčrpen seznam, temveč samo kratek opis, kaj je in kaj ni na voljo, katera orodja se lahko in katera se ne morejo uporabiti, namen/cilj preizkusa ter načrtovan čas okrevanja.

Namen testiranja je potrditev celotnega načrta okrevanja po nesrečah. Vendar testiranje ne sme biti pretežko med začetnimi fazami. Med začetnimi fazami lahko zapleteni preizkusi, ki še niso bili testirani, samo še odložijo potrditev celotnega načrta okrevanja po nesrečah ter po nepotrebnem trošijo vire organizacije.

Kriteriji preizkušanja
Vsi preizkusi ne potrebujejo prisotnosti vseh zaposlenih. Kriteriji preizkušanja določijo za sodelujoče v preizkusu, tudi opazovalce, kdaj in kje je njihova prisotnost potrebna ter kdaj se bo preizkus izvajal. Naloga opazovalcev je, da podajo nepristransko mnenje o preizkusu in navedejo komentarje za uspešne in neuspešne dele preizkusa ter na koncu podajo predloge za izboljšave.

Predpostavke
Za potrebe testiranja je treba navesti nekatere predpostavke. S tem se izognemo omejitvam, ki jih postavljajo drugi deli načrta okrevanja po nesrečah, ki so lahko še nepreverjeni. Predpostavke dovoljujejo, da se omejitve preizkušanja postavijo zunaj določenih meja. Naštetih je nekaj primerov predpostavk:
- vsa tehnična dokumentacija v načrtu okrevanja po nesrečah je popolna in pravilna,
- dobava vse opreme se lahko izvede v rokih, ki so določeni v načrtu okrevanja po nesrečah,
- vsi magnetni trakovi in oprema, ki je bila prenesena iz oddaljene lokacije, je popolna in delujoča.

Pogoji preizkušanj
Pred pričetkom preizkusa je potrebno preveriti, ali je načrt okrevanja po nesrečah popoln v vseh svojih delih, vključno z dodatki, na katere se sklicuje v osnovnem dokumentu. Vsaka skupina, ki sodeluje v preizkusu, mora biti poučena, kako njene naloge vplivajo na naloge drugih skupin (in obratno), kdaj in kako naj opravi svoje naloge ter katera orodja lahko uporabi pri izvajanju svojih nalog. Vsak vodja skupine mora voditi dnevnik preizkusa. Dnevnik preizkusa je namenjen kasnejšemu analiziranju preizkusa ter boljšim pripravam na prihodnje preizkuse.

Sestanki
Ne glede na to, ali je preizkus hipotetični, komponentni, modularni ali polni, je za vsakega treba organizirati sestanek. Na sestanku so pojasnjene meje preizkusa ter dana je možnost, da se razloži kakršnekoli tehnične nejasnosti v zvezi s preizkusom.

Če je preizkus kompleksnejši, je treba organizirati več sestankov. Npr. enega za pojasnitev mej preizkusa, drugega za razrešitev tehničnih nejasnosti in po možnosti še tretjega, na katerem se obvesti vodstvo podjetja o ciljih preizkusa. Od števila udeležencev na preizkusu ter kompleksnosti preizkusa je odvisno, koliko časa bo preteklo od sestanka do pričetka preizkusa. Po eni strani mora biti med zadnjim sestankom in pričetkom preizkusa dovolj časa, da se udeleženci (predvsem tehnično osebje) pripravijo na preizkus, po drugi strani pa med zadnjim sestankom in pričetkom preizkusa ne sme preteči preveč časa, tako da ostanejo ideje in naloge, zastavljene za preizkus, v glavah udeležencev sveže. Primer dnevnega reda sestanka je naveden spodaj:
- namen preizkusa,
- cilji skupin,
- scenarij nesreče,
- čas izvedbe preizkusa,
- lokacije posameznih skupine,
- omejitve posameznih skupin,

- predpostavke preizkusa,
- pogoji za posamezne skupine.

2.9.4 Analiza in zaključek preizkusa

Medtem ko je preizkus sam po sebi koristen, se njegova največja vrednost pokaže pri analizi le-tega. Ko je preizkus zaključen, se s konstruktivno analizo preizkusa in njegovih rezultatov lahko izboljša načrt okrevanja po nesrečah.

Po končanem preizkusu je treba izvesti zaključni sestanek. Na tem sestanku se podajo rezultati in ugotovitve preizkusa ter pogledi, kako izboljšati načrt okrevanja za prihodnje preizkuse. Ugotovitve razprav s sestanka se vključijo v poročilo preizkusa. Primer dnevnega reda zaključnega sestanka je naveden spodaj:
- celotna uspešnost preizkusa,
- uspešnost preizkusa po skupinah,
- opažanja,
- priložnosti za izboljšave,
- čas in kraj naslednjega preizkusa.

Vsak vodja skupine mora med izvajanjem preizkusa voditi dnevnik dogodkov. Informacije, pridobljene iz dnevnika dogodkov, ter informacije, ki so pridobljene iz analize preizkusa, so uporabljene za izdelavo poročila preizkusa. V poročilu so navedena vsa področja, kjer je možno izvesti izboljšave. Posamezna področja so nato dodeljena odgovornim osebam, ki morajo izboljšave narediti. Določi se tudi realni časovni rok za izvedbo izboljšav.

Noben preizkus se ne smatra za neuspešnega, če je le možno iz njega izluščiti informacije za izboljšave načrta okrevanja po nesrečah, pa čeprav cilji preizkusa samega niso bili doseženi (Edwards, Cooper, 1995, str. 27).

3 Vrste nadomestnih lokacij

Če je vzrok nesreče poplava, potres, požar ali orkan, potem obstaja možnost, da bo treba poslovanje deloma ali v celoti preseliti na alternativno lokacijo. V nadaljevanju so predstavljene različne vrste nadomestnih lokacij oz. druge vrste rešitev, ki zagotavljajo okrevanje v primeru uničenja primarne lokacije.

Pogodba o vzdrževanju z dobavitelji
Ta strategija je bistvenega pomena predvsem za organizacije z majhnimi informacijskimi sistemi. Pri izbiri te strategije so za okrevanje, popravilo in nadomestitev opreme odgovorni dobavitelji opreme. Če osnovna pogodba z dobavitelji ne predvideva kritja stroškov poškodb strojne opreme, ki

so jo povzročili zunanji dejavniki, kot npr. požar ali poplava, potem je potrebno to pogodbo razširiti oz. podpisati novo, v kateri bo kritje teh stroškov vključeno.

Pogodba o hitri dobavi
Organizacija lahko sklene vzdrževalno pogodbo z dobavitelji strojne opreme, v kateri se dobavitelji zavežejo, da bodo priskrbeli nadomestno strojno opremo v roku treh do petih dni. Ta strategija je primerna za organizacije, ki si lahko privoščijo nedelovanje svojega omrežja za teden dni ali dlje.

Vroča lokacija
Vročo lokacijo priskrbi in vzdržuje zunanji dobavitelj. Vroča lokacija je lokacija, opremljena z vso potrebno infrastrukturo, ki jo potrebuje organizacija za svoje delovanje. Ta oprema vključuje: vso računalniško strojno in programsko opremo, telefone, telefakse, telekomunikacijsko opremo, pisarniško opremo ter drugo. Na vroči lokaciji je pripravljen delujoč informacijski sistem, ki omogoča preklop na nadomestno lokacijo s karseda majhnim časom izpada delovanja omrežja organizacije. Da bi olajšali potovanje zaposlenih do vroče lokacije, je le-ta običajno locirana v oddaljenosti do 50 kilometrov od originalne lokacije (Hawkins, Yen, Chou, 2000, str. 228). Ker bi lahko oddaljenost alternativne lokacije vseeno predstavljala problem za zaposlene, je le-ta opremljena tudi s spalnimi prostori, tuši in kuhinjo.

Funkcija vroče lokacije je tudi, da omogoča zaposlenim praktičen preskus postopkov med načrtovanjem okrevanja po nesrečah. Vodilni delavci lahko preizkušajo načrt okrevanja po nesrečah v okolju, ki ne vpliva na delovanje ostalih poslovnih funkcij organizacije.

Hladna lokacija
Hladna lokacija je prazna poslovna stavba, v kateri so napeljani omrežni kabli, vodi električne energije in klima ter je pripravljena na priklop računalnikov. Ker v primeru nesreče potrebuje organizacija določeno časovno obdobje, da opremi hladno lokacijo, je le-ta primerna samo za organizacije, ki si lahko privoščijo določeno časovno obdobje brez normalnega delovanja.

Mnoge organizacije uporabljajo svoje jedilnice kot hladne lokacije na primarni lokaciji, ali pa skladišča kot hladne lokacije na oddaljeni lokaciji. V primeru, ko nesreča uniči hladno lokacijo organizacije, pa lahko organizacija najame hladno lokacijo od specializiranih dobaviteljev le-teh.

Vendar ima izbira hladne lokacije kot strategije tudi svoje slabosti. Ker je potrebno računalniško opremo prepeljati na hladno lokacijo, je potrebno usklajeno sodelovanje med varnostnim oddelkom organizacije in dobavitelji, da se zagotovi varna in hitra dobava. Zagotovitev nadomestne opreme pa lahko traja dalj časa, kar še podaljša čas nedelovanja informacijskega sistema.

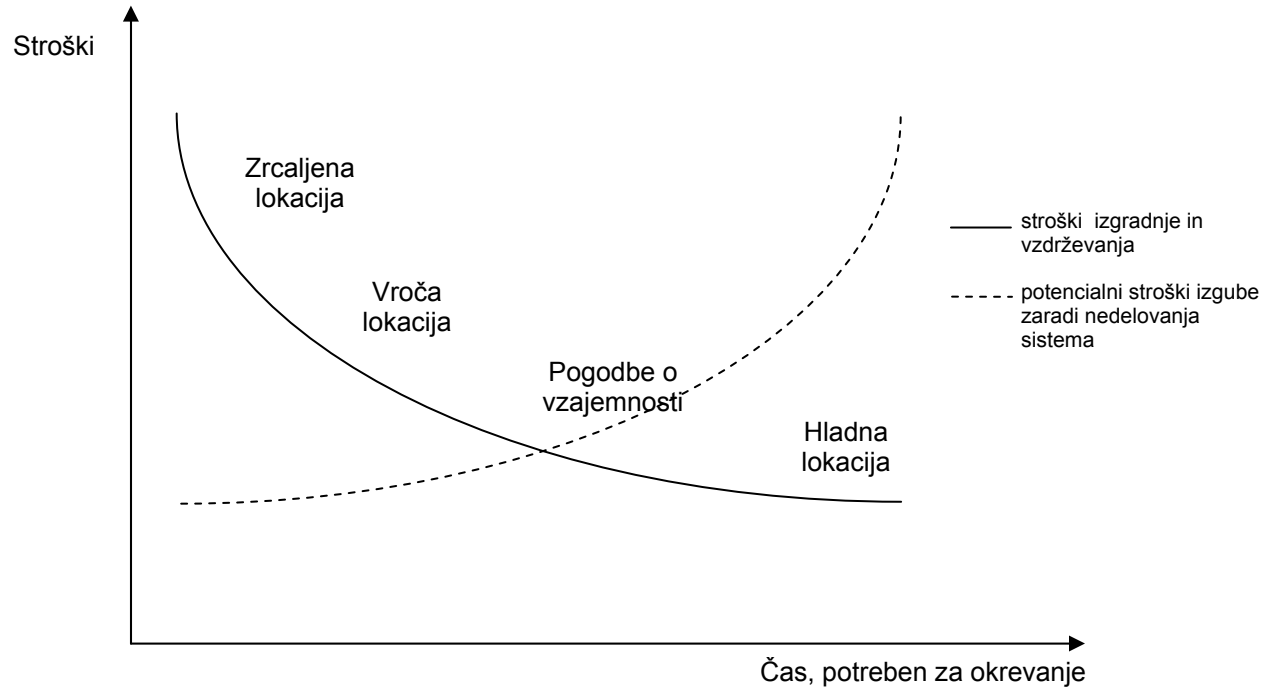
Mobilna enota za okrevanja
Mobilna enota za okrevanje je samozadostna mobilna prikolica ali zabojnik, v katerega je vgrajena potrebna računalniška oprema. Večina takšnih enot je opremljena tudi s samostojnim električnim generatorjem.

Zrcaljena lokacija
Podobno kot vroča lokacija je tudi zrcaljena lokacija opremljena z vso strojno, programsko in telekomunikacijsko opremo, ki je potrebna za takojšen prenos poslovanja na to lokacijo. Ker so organizacije večinoma lastniki teh lokacij, se podatki iz glavne lokacije neprestano prepisujejo na zrcaljeno lokacijo. Tako je zrcaljena lokacija na voljo v trenutku in z vsemi potrebnimi podatki, ko se na glavni lokaciji zgodi nesreča. Uporabniki prehoda na zrcaljeno lokacijo ne zaznajo.

Nekatere organizacije pa pošiljajo na zrcaljeno lokacijo kopije trakov nočnih varnostnih kopij. V tem primeru morajo v primeru nesreče na zrcaljeno lokacijo prenesti še podatke o transakcijah zadnjega dne. S tem se aktivacija zrcaljene lokacije nekoliko zavleče, vendar je običajno čas krajši od enega dneva.

Pogodbe o vzajemnosti
Dve organizaciji s podobnimi konfiguracijami sistemov se dogovorita, da bosta v primeru nesreče druga drugi služile kot rezervna lokacija.

Slika 2: Razmerje med stroški in potrebnim časom okrevanja pri različnih nadomestnih lokacijah



Vir: Introduction to Business Continuity Planning, 2002.

Kakor je razvidno s slike 2, imajo rešitve, ki omogočajo krajši čas okrevanja, višje stroške izgradnje in vzdrževanja oz. drugače povedano: pri cenejših izvedbah bodo okrevalni časi daljši. Po drugi strani pa so potencialne izgube, ki nastanejo zaradi nedelovanja sistema pri rešitvah z krajšim okrevalnim časom (dražja izgradnja in vzdrževanje) nižje, saj prekinitev poslovanja traja krajši čas. Tako vidimo, da se organizacijam z visokimi urnimi stroški nedelovanja sistema izplača izbrati nadomestne lokacije, ki imajo sicer višje stroške izgradnje in vzdrževanja, vendar pa so zato potencialne izgube ob nedelovanju sistema manjše. Po drugi strani pa se organizacijam, ki lahko ob nesreči daljše obdobje preživijo brez podatkov, ne izplača vlagati v rešitve, ki imajo visoke stroške izgradnje in vzdrževanja.

4 Stanje na področju načrtovanja okrevanja po nesrečah

Žal je večina statističnih podatkov s področja načrtovanja okrevanja po nesrečah, ki je dostopna v literaturi, slaba oz. pomanjkljiva. Zato ni niti mogoče podati natančnih ocen; kljub temu pa so podatki dovolj dobri, da z njihovo pomočjo dobimo predstavo o trenutnem stanju na področju načrtovanja okrevanja po nesrečah.

Nesreče lahko zajemajo večje geografsko področje ali pa so omejene na posamezno datoteko. Naj bo nesreča večja ali manjša, vsaka lahko povzroči veliko gospodarsko škodo podjetju, če le-to nima ustreznih načrtov za ukrepanje ob nesrečah.

V tabeli 5 je navedenih dvajset nesreč, ki so povzročile največjo škodo med leti 1900 in 2003. Kot vidimo, je med dvajsetimi nesrečami samo ena tehničnega vzroka, vse druge pa so naravne nesreče. Nesreče lahko povzročijo veliko škode ter prizadenejo veliko število ljudi. Iz tega sledi, da je priporočljivo tudi za državo pripravljati primerne načrte okrevanja po nesrečah, kot naj bi to delala podjetja zase.

Tabela 5: Dvajset nesreč z največjo povzročeno škodo med leti 1900 in 2003

Leto nesreče	Tip nesreče	Država	Območje	Število prizadetih ljudi	Škoda v mio USD
1992	neurje	ZDA	Florida, Louisiana, Bahami	250.055	30.000
1988	potres	Sovjetska zveza	Armenija, Leninakan, Kirovakan, Spitak	1.642.000	20.500
1998	poplava	Kitajska	Hubei, Hunan, Sichuan, Jiangxi, Fujian, Guanxi	238.973.000	20.000
1980	potres	Italija	Avellino, Potenza, Caserta, Naples	407.700	20.000
1991	poplava	Sovjetska zveza	regija Volgograda	40.000	19.000
1997	požar	Indonezija	Sumatra in Kalimantan	32.000	17.000
1994	potres	ZDA	okrožja Los Angeles, Ventura, Orange in San Bernardino v Kaliforniji	27.000	16.500
1995	poplava	Severna Koreja	okrožje Pakchon, provinca Chagan, Huichon, Hyangsan	5.700.000	15.000
1999	potres	Tajvan	Nantou Taichung, Nantou, Taizhong	108.664	14.100
1996	poplava	Kitajska	province Anhui, Guizhou, Hebei, Henen, Hubei, Hunan, Zhejiang, Jiangxi, Henen, Shangdong, Shanxi, Fujian, Xinjiang	154.634.000	12.600
1993	poplava	ZDA	Mississippi, Wisconsin, Iowa, Illinois, Missouri, Južna Dakota, Nebraska, Severna Dakota, Kanzas, Okhlahoma	64.700	12.000
1999	neurje	Francija	južno-zahodna in zahodna Francija	3.400.011	11.060
1999	potres	Turčija	Duzce, Bolu, Kaynasli	209.948	10.000
1995	neurje	ZDA	Indianna, Kentucky, Tennessee, Georgia, Carolina	67	10.000
2002	kemično razlitje	Španija	Galicia	734	9.960
1994	poplava	Italija	Piemont, Liguria	17.300	9.314
2002	poplava	Nemčija	Basse-Saxe, Saxe-Anhalt, Saxe, Bavarska, Baden-Wutemberg, Thuringe	330.108	9.129
1999	potres	Turčja	Izmit, Kocaeli, Yalova, Golcuk, Zonguldak, Sakarya, Tekirdag, Istanbul, Bursa, Eskisehir, Bolu	1.358.953	8.500
2002	poplava	Kitajska	province Shanxi, Sichuan, Hubei, Chongqing, Guizhou, Fujian, Jiangxi, Hunan, Guangxi, Chongqing	190.035.257	8.200
1999	poplava	Kitajska	province Anhui, Zhejiang, Jiangxi, Jiangsu, Hubei, Hunan, Guizhou, Sichuang, Chingquing in Yunnan	101.024.000	8.100

Vir: EM-DAT, 2004.

Vendar pa so podatki v tabeli 5 preveč splošni za opis problema okrevanja informacijskih sistemov v organizacijah in lahko služijo samo za predstavitev možnih razsežnosti nesreč. Za potrebe moje analize je primernejša tabla 6, kjer lahko ocenimo vpliv nesreč na organizacije (podjetja). Vidimo, da lahko ura nedelovanja za podjetje pomeni izpad dohodka do skoraj treh milijonov USD. Izpad dohodka je največji v panogi preskrbe z energijo, telekomunikacij, proizvodnje in v finančnih institucijah, najmanjše pa v gradbeništvu, medijih ter zdravstvu in turizmu. Seveda na te številke zelo vpliva velikost podjetja. Energetska podjetja in telekomunikacijska podjetja so praviloma zelo velika in zato ena ura nedelovanja takšnega podjetja pomeni velik izpad dohodka. Da bi izločili vpliv velikosti podjetja, lahko pogledamo, kakšen izpad dohodka na uro nedelovanja pade na posameznega zaposlenega. Najvišji potencialen izpad dohodka na zaposlenega imajo sektor finančnih institucij, energije in javnih gospodarskih služb, kjer izstopa sektor finančne institucije s skoraj 1100 USD dohodka na uro na zaposlenega. Najnižji potencialni izpad pa imajo sektor storitev, elektronike ter zdravstva in turizma, kjer ima slednji približno 40 USD dohodka na uro na zaposlenega.

V drugem viru (McCormack, 2003, str. 20), ki se sklicuje na isto raziskavo, pa je navedeno, kako so stroški nedelovanja sistema razporejeni glede na število organizacij:

- 46 % organizacij stane ura nedelovanja do 50.000 USD,
- 28 % organizacij stane ura nedelovanja med 51.000 USD in 250.000 USD,
- 18 % organizacij stane ura nedelovanja med 250.000 USD in 1.000.000 USD,
- 8 % organizacij stane ura nedelovanja 1.000.000 USD.

Vidimo, da ima skoraj polovica organizacij stroške nedelovanja sistema, ki so manjši od 50.000 USD, medtem ko ima samo 8 % organizacij stroške nedelovanja sistema, ki so večji od enega milijona USD.

Tabela 6: Stroški nedelovanja

Gospodarski sektor	Dohodek na uro v USD	Dohodek na uro na zaposlenega v USD
Energija	2.817.846	569,20
Telekomunikacije	2.066.245	186,98
Proizvodnja	1.610.654	134,24
Finančne institucije	1.495.134	1.079,89
Informacijska tehnologija	1.344.461	184,03
Zavarovalništvo	1.202.444	370,92
Trgovina	1.107.274	244,37
Farmacija	1.082.252	167,53
Bančništvo	996.802	130,52
Prehrambeni sektor	804.192	153,10
Potrošno blago	785.719	127,98
Kemijski sektor	704.101	194,53
Transport	668.586	107,78
Javne gospodarske službe	643.250	380,94
Zdravstvo	636.030	142,58
Metalurgija in naravni viri	580.588	153,11
Storitve	532.510	99,59
Elektronika	477.366	74,48
Gradbeništvo	389.601	216,18
Mediji	340.432	119,74
Zdravstvo in turizem	330.654	38,62
Povprečje	1.010.536	205,55

Vir: META Group v Moore, 2002, str. 18.

Iz do sedaj povedanega sledi, da predstavljajo nesreče veliko finančno obremenitev za organizacije, ki jih prizadenejo. Pričakovali bi, da ima zaradi tega večina organizacij primeren načrt za reševanje problemov, ki nastanejo ob nesrečah (kot je npr. načrt okrevanja po nesrečah). Vendar pa ima manj kot 25 % izmed največjih dva tisoč svetovnih podjetjih primeren načrt okrevanja po nesrečah, ki je delujoč, vseobsegajoč ter primerno preizkušen in se prilagaja spremembam v podjetjih (Elmerick, 2003, str. 20). Po drugi strani pa je raziskava družbe Gartner iz leta 2002 pokazala, da ima samo 35 % majhnih in srednje velikih podjetij izčrpne načrte okrevanja po nesrečah (Rike, 2003, str. 25). Iz

navedenih statistik naj bi sledilo, da ima načrte okrevanja po nesrečah več manjših in srednje velikih podjetij kot velikih podjetij. Vendar pa sta raziskavi najverjetneje neprimerljivi, saj ni znano, kaj so določili kot načrt z zadostno kakovostjo, ki so ga še šteli za ustreznega. Iz obeh statistik pa lahko povzamemo, da ima samo majhen delež podjetij primerne načrte okrevanja v primeru nesreče.

Med podjetji iz seznama Fortune 1000, ki imajo načrt okrevanja po nesrečah, pa le-ti vsebujejo varovanje različnih delov informacijskega sistema v naslednjih odstotkih (Patrowitcz v Hawkins, Yen, Chou, 2000, str. 222):

- 80 % ima načrte, ki vsebujejo varovanje njihovih podatkovnih centrov,
- 50 % ima načrte, ki vsebujejo varovanje njihovega podatkovnega omrežja in
- 35 % ima načrte, ki vsebujejo varovanje podatkov na osebnih računalnikih.

Razmerja med varovanjem različnih delov informacijskega sistema je možno razložiti z pomembnostjo podatkov, ki so na posameznem delu informacijskega sistema, ter vplivom na delovanje le-tega. V podatkovnih centrih se namreč nahajajo najpomembnejši podatki za poslovanje organizacije in brez delovanja podatkovnega omrežja lahko zastane večina poslovnih procesov, ki je odvisna od računalnikov. Po drugih virih naj bi bilo zadostno varovano samo 5 % osebnih računalnikov (Moore, 2002, str. 18).

Kakor so zgornji podatki različni v različnih virih, tako so tudi različni podatki o uspešnosti okrevanja po nesrečah. Najbolje opisuje uspešnost okrevanja rezultat raziskav družbe Gartner, ki je pokazala, da gresta dve od petih organizacij, ki jih doleti nesreča, v roku petih let v stečaj (Chen, Hicks, 2001 v Beacham, McManus, 2004, str. 46) Kakšen je ta delež za organizacije, ki imajo načrt okrevanja po nesrečah, v literaturi nisem našel.

5 Načrtovanje okrevanja po nesrečah v bankah

Banke ter finančni sektor na splošno poslujejo s podatki, ki se lahko enostavno zapišejo v digitalni obliki na računalniških medijih. Prav zaradi tega je bil ta sektor vodilen pri vpeljavi in uporabi informacijskih sistemov za podporo poslovanju. Ima pa dolga zgodovina uporabe informacijskih sistemov za posledico tudi veliko različnih računalniških platform in sistemov, ki predstavljajo velike naložbe v znanje in izkušnje.

Informacijski sistemi, ki obsegajo celotno poslovanje, so postali nujnost za velike finančne institucije. Podatki in informacije iz različnih virov morajo biti takoj na voljo ter morajo biti točni, če želi biti finančna institucija konkurenčna na trgu.

Splošna potreba, ki se pojavlja v bančnem sektorju, je konsolidacija sistemov. Podatki, ki se nahajajo na različnih sistemih, naj bi bili preneseni na en sistem, od koder bi lahko različne aplikacije in uporabniki z različnimi potrebami dostopali do njih. Pojavlja se nuja po uvedbi

informacijskih sistemov kot so skladiščenje podatkov, reorganizacija podatkov, dostop do podatkov za končne uporabnike itd. Končni rezultati segajo od preprostih poročil do podatkovnega rudarjenja.

Ocene o povzročeni škodi navajajo, da stane srednjo veliko banko vsaka ura nedelovanja približno šest milijonov USD (Petroni, 1999, str. 103). Prekinitve dobave električne energije, odpovedi strojne opreme, požari, poplave in druge nesreče prisilijo banke, da pokličejo na pomoč strokovnjake za okrevanje informacijskih sistemov približno 25-krat na leto (Petroni, 1999, str. 103). Po drugi strani pa finančne institucije v ZDA porabijo za približno 300 milijonov USD letno za najem polno opremljenih vročih lokacij (Petroni, 1999, str. 103).

Tudi država vpliva na odnos bank in drugih finančnih ustanov do načrtovanja okrevanja po nesrečah. Bankam je priporočeno, da redno revidirajo svoje sisteme, preverjajo odnose z zunanjimi partnerji ter preverjajo svoje načrte neprekinjenega poslovanja. V ZDA npr. zahteva država od vodstva bank, da:

- uvede politiko, postopke in odgovornosti za načrtovanje neprekinjenega poslovanja, ki obsega celotno podjetje,
- pregleda in odobri načrte neprekinjenega poslovanja vsako leto ter da se vse aktivnosti v zvezi s tem dokumentirajo.

Leta 1999 je večina velikih institucij zadovoljivo izpolnjevala zahteve, ki jih je postavil regulator v ZDA. Manjše finančne institucije pa so morale dopolniti svoje poslovanje na tem področju. Ena izmed najpogostejših pomanjkljivosti je bila pomanjkanje izdelave varnostnih kopij osebnih računalnikov, saj je večina organizacij izdelovala samo varnostne kopije svojih strežnikov.

V Sloveniji določa pogoje poslovanja bank in hranilnic Banka Slovenije. Ta je leta 1999 na podlagi zakona o bančništvu (ZBAN) izdala "Sklep o določitvi pogojev, ki jih mora izpolnjevati banka oz. hranilnica za opravljanje bančnih oziroma drugih finančnih storitev ter o določitvi dokumentacije, na podlagi katere je mogoče ugotoviti, ali bo družba sposobna opravljati dejavnosti, na katere se nanaša zahteva za izdajo dovoljenja". V tretji točki tega sklepa določa Banka Slovenije minimalne tehnične pogoje, ki morajo biti izpolnjeni za opravljanje bančnih oz. drugih finančnih storitev. V tretji točki je določen tudi obvezujoči slovenski standard PSIST BS 7799:1997 "Kodeks varovanja informacij," ki ga morajo banke in hranilnice upoštevati pri izgradnji in varovanju informacijske tehnologije.

Standard BS 7799 predlaga procesni pristop za vzpostavitev, uvajanje, izvajanje, spremljanje, vzdrževanje in izboljševanje upravljanja sistema varovanja informacijske tehnologije. V standardu je tudi predlagan model, ki obsega naslednje korake:

- planiranje,
- uvajanje in izvajanje,
- nadzor in preverjanje (ta korak vsebuje revizijo sistema),
- vzdrževanje in izboljšave.

Po mnenju Bizjaka (2004, str. 4) je trenutni obvezujoči standard zastarel. Standard tudi ni v skladu z mednarodnim standardom ISO 17799, ki ureja področje varovanja informacijskih sistemov.

5.1 Načrtovanje neprekinjenega poslovanja: Primer Banca Commerciale Italiana

Banca Commerciale Italiana je bila ustanovljena leta 1894 (Aganin, Volpin, 2003, str. 3) in je trenutno ena izmed večjih bank v Italiji. Banka je razvila svoj aplikativni sistem, ki temelji na podatkih in ne operacijah. Aplikativni sistem podpira več platform ter sinhrone in asinhrone aplikacije. Rešitev je dovolj prilagodljiva, da podpira različne načine komunikacij: X.25, TCP/IP in SNA/APPC, potrebne za programsko opremo za obdelavo transakcij banke. Pred vpeljavo novega sistema so se vse obdelave izvajale na osrednjem računalniku. Sedaj imajo vse aplikacije enak zunanji izgled. Imajo povezave do zunanjih ponudnikov informacij, kot npr. do Reutersa, do notranjih in zunanjih trgov vrednostnih papirjev itd. Nekatere interne aplikacije za svoje delovanje potrebujejo informacije, ki jih nudijo zunanji ponudniki informacij. Imajo razvit tudi sistem distribuiranja aplikacij do več kot deset tisoč uporabnikov. Zagotovljena je dostava informacij iz različnih delov informacijskega sistema do drugih delov, z uporabo vrst, varnostno politiko, orodji za zagotavljanje integritete podatkov, izdelavo dnevnikov, sledljivostjo ter izdelavo varnostnih kopij.

Banca Commerciale Italiana mora tako kot tudi druge finančne institucije zagotoviti neprekinjeno delovanje obdelave podatkov in drugih kritičnih funkcij. Da bi se izognili motnjam (oz. zmanjšali njihov vpliv), je banka leta 1992 začela izdelavo načrta neprekinjenega delovanja. Ta načrt se je predvsem osredotočil na postopke okrevanja in fizično premestitev podvojenih komponent informacijskega sistema. Odgovornost za projekt je bila dodeljena skupini za "Zdravje informacijskih sistemov." Naloga skupine je bila zagotovitev učinkovitega in varnega transakcijskega procesiranja, upravljanja s podatki in storitev, ki jih ponujajo svojim strankam, ter drugim organizacijam.

Vodilo, ki ga je vodstvo banke izbralo za zmanjšanje prekinitev v delovanju sistema, je vključevalo:
- ustanovitev skupine za krizno vodenje, katere člani so imeli točno določene odgovornosti,
- ocenitev stroškov prekinitve delovanja sistema na uro, na dan in na teden ter
- določitev ključnih informacij, ki morajo biti neprestano na voljo.

Čeprav so bile razvite dobre metode za upravljanje z ranljivostmi informacijskega sistema, le-te niso mogle nadomestiti načrta okrevanja po nesrečah. Zaradi tega so se odločili, da morajo razviti tudi strategijo okrevanja po nesrečah, ki bo vsebovala naslednje korake:
- določitev grožnje za lokacije, kjer so locirani kritični podatki,
- izdelava varnostnih kopij podatkov ter redno preverjanje, ali so bile varnostne kopije podatkov narejene uspešno,
- preverjanje, ali so bili podatki uspešno preneseni na nadomestno lokacijo,

- redno prenašaje varnostne kopije na nadomestno lokacijo,
- hranjenje pomembnih dokumentov na alternativni lokaciji,
- določitev najboljše lokacije in metode za okrevanje operacij,
- dokumentiraje načrta okrevanja po nesrečah z uporabo namenske programske opreme,
- preizkus načrta okrevanja po nesrečah vsaj dvakrat letno, ter istočasna obnovitev načrta.

Naslednji korak je bila izdelava celotnega načrta neprekinjenega delovanja omrežja. Načrt neprekinjenega delovanja omrežja naj bi dosegel naslednje štiri cilje:
- zagotovitev neprekinjenega delovanja organizacije,
- minimiziranje časa obnovitve,
- podpora širšemu načrtu okrevanja poslovanja po nesrečah ter združitev z obstoječimi načrti informacijskega sistema,
- zadovoljitev vseh pravnih zahtev, ki jih določa država in njeni organi.

Normativi, ki sta jih v tistem času določala Evropska unija ter Banca d'Italia, so bili zelo strogi. Namen regulativ je bil zagotoviti medbančne poravnave. Za majhne banke ter za kratke prekinitve, so lahko bile izgube iz tega naslova majhne, vendar so za večje banke, kot je npr. Banca Commerciale Italiana, lahko izgube že ob majhnih prekinitvah velike. Banca Commerciale Italiana ima dnevne transakcije, ki vrednostno znašajo več tisoč milijonov USD, tako da lahko ob dnevni prekinitvi samo penali nanesejo več milijonov USD.

V jedru je bil celoten proces sestavljen iz poglobljene analize najbolj kritičnih poslovnih funkcij organizacije, sestavi strategij okrevanja, vse skupaj pa je bilo zapisano v lahko razumljiv dokument. V dokumentu so zapisane naloge in odgovornosti osebja za primer okrevanja. Banca Commerciale Italiana je vključila sledeče elemente v svoj načrt okrevanja po nesrečah:
- načrti ukrepanja ob incidentih,
- okrevalni načrti informacijskega sistema ter delovnih skupin,
- nadomestne možnosti za izvajanja poslovanja,
- revizije varnostnih postopkov,
- analiza varovanja podatkov,
- preizkušanje okrevanja ter program vzdrževanja načrta okrevanja po nesrečah.

Načrtovanje neprekinjenega delovanja je bilo razvito z uporabo metode življenjskega cikla. Metoda življenjskega cikla, ki so jo uporabili v Banca Commerciale Italiana, vsebuje tri faze:
1. Analiza sistema, ki je ena izmed najpomembnejših faz izgradnje načrta neprekinjenega delovanja, saj vsebuje določitev ter ocenitev izpostavljenosti ter določitev prioritet za intervencijo. Analiza okrevanja omrežja je vsebovala postopke izdelave varnostnih kopij, začasno opremo, telekomunikacije, določitev prioritet aplikacij ter hranjenje kritičnih podatkov in materialov na oddaljeni lokaciji.

2. Design sistema: V tej fazi je morala skupina, zadolžena za neprekinjeno delovanje, upoštevati podvojevanje komponent sistema ter izdelavo varnostnih kopij.
3. Implementacija sistema.

Načrt sistema in implementacija

Zamenjava celotnega lokalnega omrežja ni bila ekonomsko smiselna, zato so morali vodilni delavci banke pretehtati faktorje stroškov in ranljivosti med izdelavo načrta okrevanja po nesrečah. Drugače povedano: vodilni delavci banke so morali pregledati tveganja ter vsakega oceniti glede na:

- verjetnost dogodka,
- vpliv na tekoče operacije organizacije.

Kar zadeva vpliv na tekoče operacije, sta bila upoštevana dva enakovredna faktorja: kapacitete obdelave podatkov ter hitrost časovne razpoložljivosti informacij, čeprav je zelo težko določiti, kaj pomeni prekinitev delovanja sistema, saj dnevno informacijski sistem procesira več kot dva milijona sporočil. Prav tako je težko določiti zmanjšanje storitev za stranke, saj ima Banca Commerciale Italiana približno šestnajst tisoč oddaljenih naprav (od elektronskih blagajn do POS-ov ipd.)

Pri implementaciji načrta okrevanja po nesrečah se je moralo vodstvo odločati med alternativnimi rešitvami. Na razpolago so imeli več različnih načrtov sistemov, primernih za izvedbo podvojevanja:

- Načrt A: Celotna obdelava podatkov (100 %) se izvaja na eni procesni enoti, ki je locirana v Parmi. Sistematično se izdelujejo varnostne kopije, ki se prenašajo na drugo enoto (locirano v Milanu). Druga enota je v stanju pripravljenosti ter ima določeno zmogljivost obdelave podatkov, ki se aktivira ob aktivaciji postopka iz načrta okrevanja po nesrečah. V primeru izgube celotne procesne enote se na drugi lokaciji naredi obnova podatkov iz varnostnih kopij, ki so bile narejene dan pred nesrečo ("hladna obnova") ter se nato požene postopek obnovitve preostalih podatkov, kar se lahko izvede v približno 36 urah.
- Načrt B: Enako kot načrt A, samo z "vročo obnovo" podatkov, kar pomeni uporabo sistema, ki zrcali podatke v realnem času iz glavne procesne enote na oddaljeno enoto z uporabo hitrih omrežnih povezav. Takšni sistemi so lahko obnovljeni v 45 minutah brez izgube podatkov.
- Načrt C: Dve ločeni procesni enoti za obdelavo podatkov, locirani na dveh različnih delih iste lokacije (Parma) ter povezani med sabo s hitrimi omrežnimi povezavami. Takšen sistem omogoča vzporedno obdelavo podatkov na obeh enotah ter stalno (obojestransko) izmenjavo podatkov med enotami v realnem času. Kapaciteta obdelave podatkov je razdeljena med obema enotama v razmerju 60:40. Dnevno se izdeluje varnostna kopija, ki se prenaša na rezervno enoto, ki je locirana v drugi stavbi. Rezervna enota se uporablja za "hladno obnovo" v primeru, da sta poškodovani obe procesni enoti. V primeru poškodbe ene od glavnih procesnih enot pa prevzame obdelavo (ter vse podatke) druga (glavna) procesna enota.
- Načrt D: Isto kot načrt C, samo z "vročo obnovo."

Določitev zanesljivosti sistema

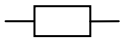
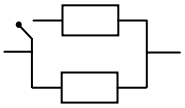
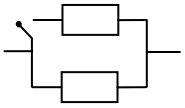
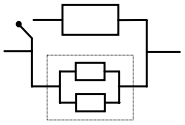
Ena izmed najpomembnejših nalog vodstva banke je bila merjenje zanesljivosti. Del vodstva, ki je zadolžen za informacijske sisteme, je moral oceniti, kateri načrti sistemov, primernih za izvedbo podvojevanja, so primerni za določene vrste tveganja ter kateri so neprimerni za določene vrste tveganja. Potrebovali so orodje za primerjalno analizo prednosti in slabosti štirih možnih načrtov sistemov, primernih za izvedbo podvojevanja, v perspektivi koristi/stroški. Za analizo so uporabili metodo, ki temelji na verjetnostni učinkovitosti in ima teoretične osnove v teoriji zanesljivosti sistemov. Osnovno predstavitev metode lahko bralec najde v Petroni (1999, str. 109).

Takšno metodo so želeli na koncu uporabiti za računanje učinkovitosti celotnega sistema ter posledično stroške prekinitve delovanja sistema. Zato so upoštevali različne vsebinske pogoje (takšne z večjim vplivom na obnašanje sistema in takšne z vplivom na zanesljivost sistema):

- možna izpostavljanja tveganju in dogodki izgube, katerim so sistemske enote najbolj izpostavljene, saj te vplivajo različno na logično obnašanje sistema. Zaradi tega so bili tipi izpostavitve tveganju združeni v tri skupine glede na verjetnost, da se pripetijo, ter njihov skupni vpliv na sistemske vire. Hipotetični katastrofalni dogodki so bili združeni v tri osnovne topologije glede na verjetnost, da se pripetijo, ter glede na njihov relativni vpliv na sistem. Sistemska logika obnašanja se spreminja glede na tipe dogodkov, kot je prikazano v tabeli 7.
- Pomembnost za delovanje potencialnih podsistemov (npr. kapacitete obdelave proti razpoložljivosti sveže obnovljenih podatkov).

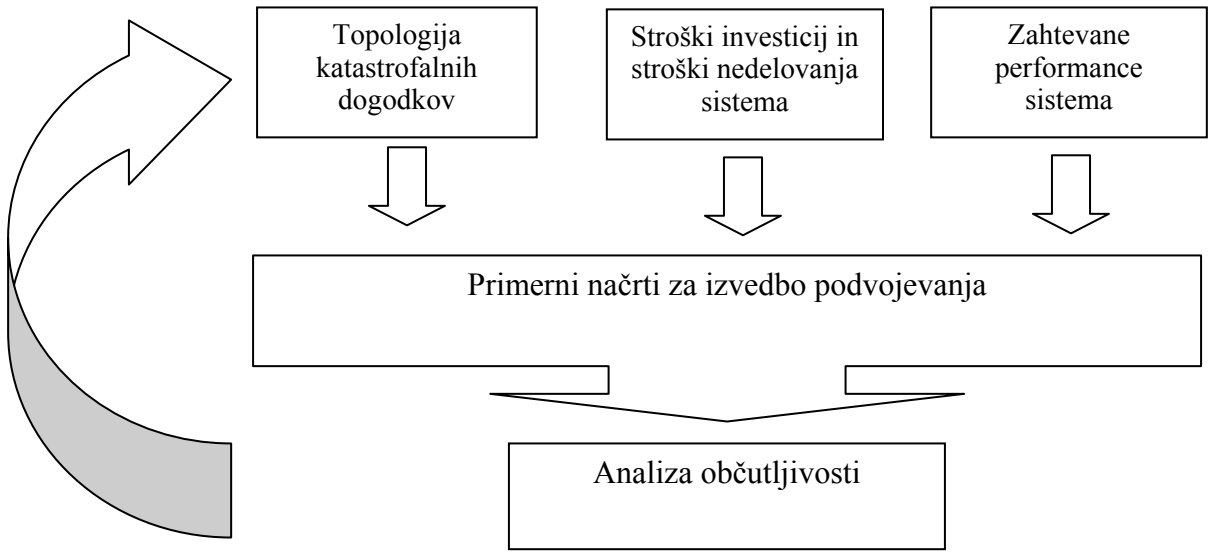
To metodo so implementirali v računalniški simulaciji, katere namen je bil izdelava analize občutljivosti s spreminjanjem začetnih pogojev tipov tveganja in pomembnosti za delovanje sistema. Grafično je to predstavljeno na sliki 3.

Tabela 7: Katastrofalni dogodki in logično obnašanje konfiguracij načrtov okrevanja

Tip dogodka	**Primeri**	**Logično obnašanje konfiguracij načrtov okrevanja**
I Tveganja na širšem geografskem območju ocenjena frekvenca dogodkov 1/1000 [1/leto]	– potres na širšem območju, – eksplozija atomske bombe, – koordiniran teroristični napad	Za vse 4 konfiguracije: preprost sistem 
II Tveganja na omejenem geografskem območju ocenjena frekvenca dogodkov 1/1000 [1/leto]	– potres na omejenem območju, – poplava, tornado, – požar, – usmerjen teroristični napad	Za vse 4 konfiguracije: dva vzporedna elementa z zaporednimi operacijami in preprostim podvajanjem 
III Lokalna tveganja ocenjena frekvenca dogodkov 1/1000 [1/leto]	– lokalni požar, – razlitje vode, – računalniški kriminal	A in B konfiguracije: enako kot tip II dogodka  C in D konfiguracije: dva vzporedna elementa s stalnimi operacijami ter tretji element vzporedno z zaporednimi operacijami 

Vir: Petroni, 1999, str. 107.

Slika 3: Teoretični načrt analize



Vir: Petroni, 1999, str. 107.

V prvem delu analize so hoteli določiti celotne stroške prekinitve poslovanja. To je bila pomembna in težka naloga, saj se je izkazalo, da je težko natančno izmeriti dodatne stroške zaradi nakupa dodatne opreme, procesorjev itd., zaradi zagotovitve zadovoljivega podvojevanja ter zamenjave pokvarjene opreme.

V drugem delu analize pa so izvedli analizo občutljivosti, ki je bila izvedena s spreminjanjem pomembnosti delovanja različnih podsistemov.

Oba dela analize sta podprla hipotezo, da je načrt izvedbe D najprimernejši za okolja, kjer je velika pomembnost določena dnevni razpoložljivosti novih podatkov (kar je vsekakor pravilna predpostavka za veliko banko).

Vodstvo banke se je zato odločilo za načrt izvedbe D: dve samostojni ter ločeni lokaciji, na katerih je identična oprema (ena v Milanu, druga v Parmi). Lokaciji sta povezani s hitrimi omrežnimi povezavami. To omogoča dostop do podatkov na računalnikih na obeh lokacijah ter hiter prehod na obdelavo na drugi lokaciji, če se na eni zgodi nesreča.

Prednosti izbrane rešitve sta dveh vrst. Kot prvo, omogoča podvojena oprema povečanje učinkovitosti obdelave podatkov, tako da se prenaša obdelava podatkov dinamično na trenutno najprimernejši del sistema, ter lažjo in hitrejšo obdelavo podatkov ob najbolj obremenjenih delih dneva. Kot drugo, omogoča ta rešitev t.i. "vročo obnovo", kar pomeni, da lahko v primeru popolnega uničenja ene od lokacij sistem popolnoma obnovijo v manj kot petinštiridesetih minutah.

6 Sklep

Res je, da daje vsako opustošenje možnost za nov začetek, vendar je velika razlika med opustošenjem, ki uniči poslovno zgradbo organizacije, in opustošenjem, ki popolnoma uniči vse podatke organizacije. Če je imela organizacija v prvem primeru primerno zavarovanje ali zadostne finančne rezerve, lahko zgradi novo zgradbo ter obnovi svoje poslovne procese. Popolnoma uničenih podatkov pa se ne da nadomestiti in ta scenarij pomeni zagotovo prenehanje delovanja organizacije.

Dandanes večina poslovnih procesov poteka s pomočjo računalnikov, odvisnost od informacijske tehnologije pa se bo samo še večala. V današnji dobi je skoraj vsako podjetje ali organizacija odvisna od podatkov na računalniških medijih ter procesov, ki se izvajajo s pomočjo računalnikov. Naj gre za majhno podjetje ali mednarodno podjetje, nihče si ne more privoščiti izgube podatkov oz. nedelovanja svojega informacijskega sistema, saj lahko to resno ogrozi njegov obstoj.

Informacijski sistemi znotraj organizacij pa tudi med organizacijami se vedno bolj povezujejo. Zato postajajo poslovni procesi vedno bolj odvisni od njih. Če preneha delovati ključni del informacijskega sistema, pa naj bo ta še tako majhen, bodo vsi deli, ki so od njega odvisni, nehali delovati. In trend povezovanja ter posledično odvisnosti se bodo samo še nadaljevali. Prav zato morajo organizacije s pravilnimi ukrepi zagotoviti, da bo njihovo poslovanje kar najmanj moteno, čeprav bodo deli informacijskih sistemov še naprej odpovedovali.

Ne glede na to, da segajo prvi začetki varovanja informacijskih sistemov v šestdeseta leta dvajsetega stoletja ter da so poslovni procesi organizacij vedno bolj odvisni od informacijskih sistemov in od podatkov na računalniških medijih, stanje varovanja le-teh ni na takšni ravni, kot bi pričakovali.

Trenutno stanje varovanja informacijskih sistemov sploh ni zadovoljivo. Vpeljava načrtovanja okrevanja po nesrečah je v podjetjih izjema in ne pravilo. Večina podjetij namreč še vedno nima nikakršnega načrta za obnovitev poslovanja v primeru nesreče. Očitno se vodilni delavci še ne dovolj zavedajo vrednosti podatkov ali pa ne vedo, da se nesreče neprestano dogajajo (naravne, nesreče tehničnega vzroka ali pa človeškega vzroka) ter da informacijski sistemi niso imuni na nesreče. Pričakujemo lahko, da se bo stanje varovanja informacijskih sistemov v prihodnosti povečalo ter da bo tovrstno varovanje nekoč postalo tako samoumevno, kot je danes fizično varovanje premoženja podjetja. V marsikaterem podjetju so namreč podatki vredni več, kakor njihovo fizično premoženje.

Ostaja pa vprašanje, zakaj se bodo podjetja odločila vpeljati sistem varovanja. Institucijam, ki so pomembne na nacionalni ravni, že danes država predpisuje načine in stopnje varovanja in te nimajo izbire – varovanje morajo uvesti. Druge organizacije pa so danes prepuščene lastni odločitvi. Za odločitev o varovanju podatkov bo pri teh organizacijah odločala bodisi večja zavest o pomembnosti varovanja informacijskih sistemov bodisi nesreča, v kateri se bo pokazala ranljivost nevarovanega informacijskega sistema (pri čemer nesreča ne bo prevelika, da bi organizacija zaradi nje propadla). Naravna selekcija bo tudi poskrbela, da po večji nesreči, podjetij brez ustreznega varovanja ne bo več.

Danes poteka varovanje večinoma samo na najpomembnejših delih informacijskega sistema, kot so strežniki in podatkovna središča. Drugi deli informacijskega sistema so večinoma zanemarjeni, čeprav lahko tudi ti vsebujejo pomembne informacije za delovanje organizacije ali pa informacije o tem, na kakšen drug način vplivajo na poslovne procese. V organizacijah, katerim država predpisuje načine varovanja, so zavarovani vsi deli informacijskega sistema; pričakujemo pa lahko, da se bo varovanje tudi v drugih organizacijah v prihodnosti razširilo na vse dele informacijskih sistemov. Varovani bodo tako najpomembnejši strežniki kot osebni računalniki, v prihodnosti pa tudi druge naprave (npr. dlančniki, mobilniki itd.)

Na področju načrtovanja okrevanja po nesrečah čakajo večino organizacij še veliki izzivi in veliko dela. In prav od tega bo odvisno, ali bodo organizacije naslednjo večjo nesrečo preživele ali ne.

7 Literatura

1. Aganin Alexander, Volpin Paolo: The History of Corporate Ownership in Italy. [URL: http://faculty.london.edu/pvolpin/history.pdf], oktober 2003, str. 1 - 45.
2. Bahan Chad: The Disaster Recovery Plan [URL: http://www.sans.org/rr/papers/16/1164.pdf], junij 2003.
3. Bizjak Miran: Varovanje v telekomunikacijah – upravljalski proces. [URL: http://www.lfte.org/pdf/Varovanje%20v%20telekomunikacijah.pdf], 14.8.2004.
4. Chow S. Wing: Success factors for IS disaster recovery planning in Hong Kong. Information Management & Computer Security, B. k., 2000, 8/2, str. 80 – 86.
5. Davis Steve: Developing Continuity in Government Planning. Disaster Recovery Journal. Spring 2003. [URL: http://www.drj.com/articles/spr03/1602-01p.html]
6. Edwards Bruce, Cooper John: Testing the disaster recovery plan. Information Management & Computer Security, B. k., 3 (1995) 1, 3/1, str. 21 – 27.
7. Elmerick Mark: Disaster Recovery Planning: Are you prepared? The Secured Lender, B.k., 2003, november/december, str. 20 – 24.
8. Hawkins Steve M., Yen David C., Chou David C.: Disaster recovery planning: a strategy for data security. Information Management & Computer security, B. k., 2000, 8/5, str. 222 – 229.
9. Lee Sooun, Ross Scott: Disaster Recovery Planning for Information Systems. Information Resources Management Journal, B. k., 1995, Summer, str. 18 – 23.
10. McCormack John: When Data Equals Dollars, Time Is Of The Essence. Processor, B.k., Volume 25, 25 (2003) 49, str. 20.
11. McManus Deniese Johnson, Beacham Alyson E.: Recovery of Financial Services Firms in the World Trade Center, Post 9/11/01. Information System Security, B.k., 2004, maj/junij, str. 46 – 54.
12. Moore Fred: Backup is Important, Recovery is Everything. Computer Technology Review, B.k., 2002, marec, str. 1 – 20.
13. Petroni Alberto: Managing information systems' contingencies in banks: a case study. Disaster Prevention and Management, B. k., 8 (1999) 2, str. 101 – 110.
14. Rike Barb: Prepared or not... that is the vital question. Information Management Journal, B.k., 2003, maj/junij, str. 25 - 33.

8 Viri

1. EM-DAT: The OFDA/CRED International Disaster Database [URL: http://www.em-dat.net/disasters/list.php], 26.8.2004.
2. Herman Eric, Neumeier Brett: Single Point Of Failure [URL: http://c2.com/cgi/wiki?SinglePointOfFailure], 14.8.2004.
3. SANS Institute: Introduction to Business Continuity Planning [URL: htttp://www.sans.org/rr/papers/16/559.pdf], 2002.

4. Sklep o določitvi pogojev, ki jih mora izpolnjevati banka oz. hranilnica za opravljanje bančnih oziroma drugih finančnih storitev ter o določitvi dokumentacije, na podlagi katere je mogoče ugotoviti, ali bo družba sposobna opravljati dejavnosti, na katere se nanaša zahteva za izdajo dovoljenja (Uradni list RS, št. 7/99).

9 Slovar tujk

best case for staffing scenario – najboljši scenarij za osebje
business continuity planning – načrtovanje neprekinjenega poslovanja
bussines resumption plan – načrt obnovitve poslovanja
cold site – hladna lokacija
comprehensive emergency management program – splošen vodstveni načrt za izredne razmere
continuity of operations plan – načrt neprekinjenega delovanja
critical – kritično(uporabljeno pri razvrstitvi delov informacijskega sistema)
disaster – nesreča
disaster recovery planning – načrtovanje okrevanja po nesrečah
essential – bistveno (uporabljeno pri razvrstitvi delov informacijskega sistema)
hot site – vroča lokacija
incident management plan – načrt ravnanja ob incidentih
logical support team – skupina za logistično podporo
mainframe – osrednji računalnik
mirrored site – zrcaljena lokacija
mission critical– kritično za poslanstvo (uporabljeno pri razvrstitvi delov informacijskega sistema)
non–critical – nekritično (uporabljeno pri razvrstitvi delov informacijskega sistema)
occupant emergency plan – načrt zaščite in reševanja
recovery operations team – skupina za obnovitev procesov
recovery point objective – kritična obnovitvena točka
recovery strategy – strategija obnovitev
recovery time objective – kritični obnovitveni čas
redundand array of independent disks – skupina neodvisnih diskov s preobiljem podatkov
response team – odzivna skupina
restoration – obnova
restoration team – obnovitvena skupina
single point of failure – posamezna točka napake
system recovery time – čas okrevanja sistema
worst case for staffing scenario – najslabši scenarij za osebje
worst case scenario – najslabši scenarij