Upravljanje kontinuitetom poslovanja u kontekstu izoliranog informacijskog sustava

Račić, Ivan

Sveučilište u Zagrebu

FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Ivan Račić

UPRAVLJANJE KONTINUITETOM POSLOVANJA U KONTEKSTU IZOLIRANOG INFORMACIJSKOG SUSTAVA

SPECIJALISTIČKI RAD

Zagreb, 2021.

Sveučilište u Zagrebu

FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Ivan Račić

UPRAVLJANJE KONTINUITETOM POSLOVANJA U KONTEKSTU IZOLIRANOG INFORMACIJSKOG SUSTAVA

SPECIJALISTIČKI RAD

Zagreb, 2021.

Završni specijalistički rad izrađen je na Sveučilištu u Zagrebu Fakultetu elektrotehnike i računarstva, na Zavodu za primijenjeno računarstvo.

Mentor: prof. dr. sc. Krešimir Fertalj, Zavod za primijenjeno računarstvo

Završni rad ima: 85 stranica

Završni rad br.:

Povjerenstvo za ocjenu u sastavu:

1. Prof. dr. sc. Nikola Hadjina, Zagreb - predsjednik
2. Prof. dr. sc. Krešimir Fertalj - mentor
3. Prof. dr. sc. Neven Vrček, Sveučilište u Zagrebu Fakultet organizacije i informatike – član.

Povjerenstvo za obranu u sastavu:

1. Prof. dr. sc. Nikola Hadjina, Zagreb - predsjednik
2. Prof. dr. sc. Krešimir Fertalj - mentor
3. Prof. dr. sc. Neven Vrček, Sveučilište u Zagrebu Fakultet organizacije i informatike – član.

Datum obrane: 26. listopada 2021.

Sadržaj

1. Uvod

U poslovnom okruženju bilo kakve poslovne organizacije – poduzeća, neprofitne udruge, državnog tijela, mogu se pojaviti razni neočekivani štetni događaji koji mogu prekinuti poslovanje na kraće ili duže vrijeme. Prijetnje koje izazivaju takve događaje javljaju se u rasponu od prirodnih katastrofa poput poplave ili potresa, preko ljudskog djelovanja poput kibernetičkog napada do tehničkih problema poput nestanka električnog napajanja. One mogu djelovati na razne aspekte poslovanja od, primjerice, fizičkog uništenja skladišta s robom zbog požara, preko epidemije koja je onesposobila cijeli odjel prodaje do nestanka struje zbog kojeg su izgubljeni važni podatci u informacijskom sustavu organizacije. Iz tog razloga u organizaciji je potrebno razviti plan to jest procedure kojima će se u takvim izvanrednim situacijama nastaviti poslovanje.

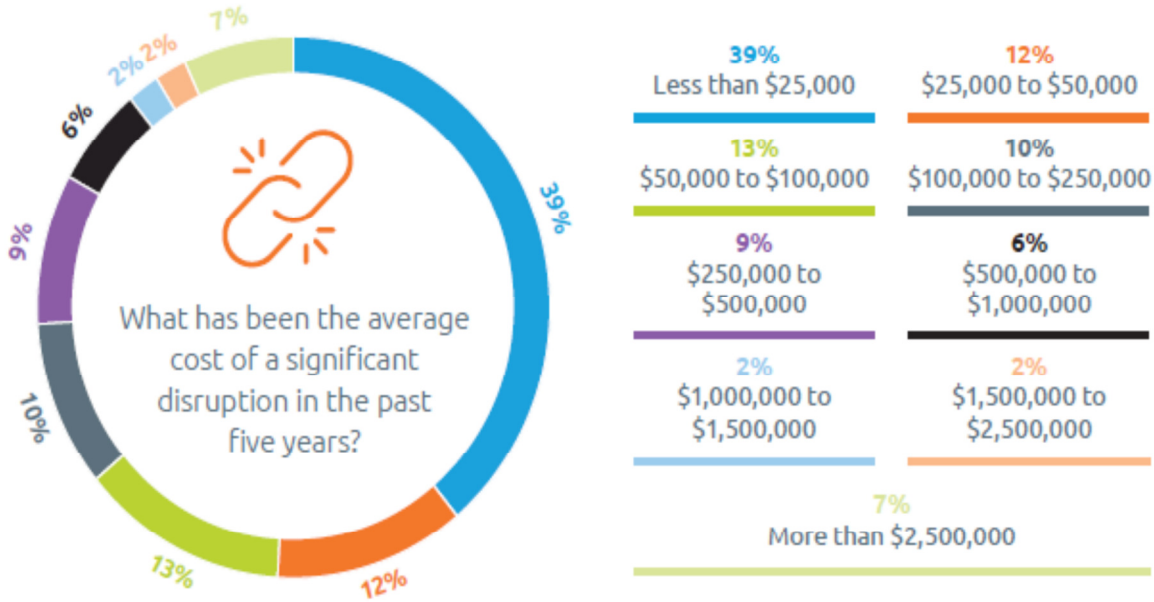
Organizacije u suvremenom poslovanju uglavnom koriste informacijske sustave koji imaju priključak na Internet. Međutim, određena vojna, financijska, industrijska te druga osjetljiva poslovna okruženja (zdravstvo, zračni promet, nuklearne elektrane) imaju potrebu za korištenjem izoliranih informacijskih sustava. To su sustavi koji u cilju povećanja sigurnosti od kibernetičkih napada i zaštite klasificiranih podataka koji su sadržani u njima nemaju mrežnu povezanost s drugim sustavima kao što je Internet ili druge nesigurne mreže. S obzirom da je suvremeno poslovanje svih organizacija u velikom dijelu oslonjeno na informacijske sustave, nužno je da oni budu stalno dostupni korisnicima zbog čega je potrebno razviti planove i procedure upravljanja kontinuitetom poslovanja. Ono se u načelu ne razlikuje od upravljanja kontinuitetom poslovanja na bilo kojem drugom sustavu te također obuhvaća analizu utjecaja na poslovanje, upravljanje rizicima te oporavak od katastrofe. Ono u čemu su izolirani sustavi specifični je podskup ovog posljednjeg odnosno oporavak od katastrofe u IT području. Budući da izolirani informacijski sustav nije povezan na Internet ni na druge mreže, nema mogućnosti pohrane podataka ili uporabe poslužiteljskih i aplikacijskih resursa izvan organizacije, primjerice u oblaku (engl. cloud). Također nema mogućnosti prebacivanja brige za oporavak od katastrofe na vanjsku uslugu (engl. Disaster Recovery as a Service, DRaaS). Organizacija u kojoj se izolirani informacijski sustav nalazi mora imati vlastitu IT infrastrukturu (poslužitelji, aplikacije, uređaji za pohranu podataka, mrežni uređaji)

te uspostaviti redundantnost iste na udaljenoj lokaciji. Za takvu organizaciju je oporavak od katastrofe u IT području najosjetljiviji segment upravljanja kontinuitetom poslovanja kojem se treba posvetiti posebna pažnja. Ukoliko se o tome ne vodi računa, katastrofa poput požara ili poplave može bespovratno uništiti podatke i aplikacije koje izolirani sustav sadrži što bi nanijelo nepopravljivu štetu poslovanju organizacije, a moguće i opasnost za ljudske živote ako se primjerice radi o sustavu koji se nalazi u zdravstvu ili kontroli zračnog prometa.

2. Planiranje za nepredviđene okolnosti

Sve organizacije se svakodnevno suočavaju s nizom vanjskih i internih rizika to jest nepredviđenih okolnosti koji mogu izazvati štetu za poslovanje organizacije. Jedno globalno istraživanje provedeno 2010. godine na više od 200 kompanija u Institutu za kontinuitet poslovanja, Bussiness Continuity Institute (BCI) pokazalo je da je oko 34% svih organizacija iskusilo dva ili više neočekivanih štetnih događaja unutar jedne godine [**1**]. Većina takvih događaja nisu katastrofalnih razmjera, ali i događaji poput privremenog nestanka električne energije ili kvara poslužitelja mogu privremeno zaustaviti poslovanje, a u najgorem slučaju oštetiti najveće vrijednosti organizacije: njeno ime i reputaciju. Uprava organizacije mora dobro razmotriti kakve su mogućnosti oporavka poslovanja u takvim situacijama te razraditi određeni plan za nepredviđene okolnosti.

Planiranje za nepredviđene okolnosti (engl. contingency planning, CP) provodi se u svrhu prilagodbe i odgovora na rizike u cilju održavanja neprekidnosti poslovnih operacija čime se osigurava rast i razvoj te prihvatljivost organizacije kao pouzdanog partnera za poslovanje. Rizici poput dugotrajnog gubitka električne energije, nedostupnosti telefonske i/ili Internetske veze, krađa važne informatičke opreme te sličnih incidenata problem su cijele organizacije. Svaki značajan prekid poslovanja može izazvati gubitak prihoda, gubitak klijenata i tržišnog udjela, globe za nesukladnost s propisima, troškove za ponovnu izradu izgubljenih podataka, troškove za prekovremeni rad osoblja koje radi na oporavku od prekida, gubitak ugleda te mnoge druge gubitke i troškove [**2**]. Planiranje za nepredviđene okolnosti predstavlja dobru poslovnu praksu koja po svom sadržaju treba imati stratešku dimenziju za poslovanje organizacije i ne treba ga shvaćati kao uski skup reaktivnih mjera na rizike odnosno incidente u poslovanju. Međutim, s obzirom na to da je izrada kvalitetnog i primjenjivog plana dosta složena te su ju uprave organizacija sklone doživljavati kao trošak, mnoge organizacije izbjegavaju njegovu izradu. Takav pristup je pogrešan. Drugo globalno istraživanje instituta BCI iz 2018. godine provedeno na preko 600 kompanija u cijelom svijetu pokazalo je kako je u prethodnih pet godina čak 26% organizacija imalo troškove u iznosu 250.000 USD i veće uzrokovane incidentima koji su privremeno onemogućili poslovanje, a prikazano je na slici 1 [**3**].



Slika 1 – Prosječan trošak uzrokovan incidentima koji su privremeno onemogućili poslovanje, 2013-2018 godina (N=627) [3]

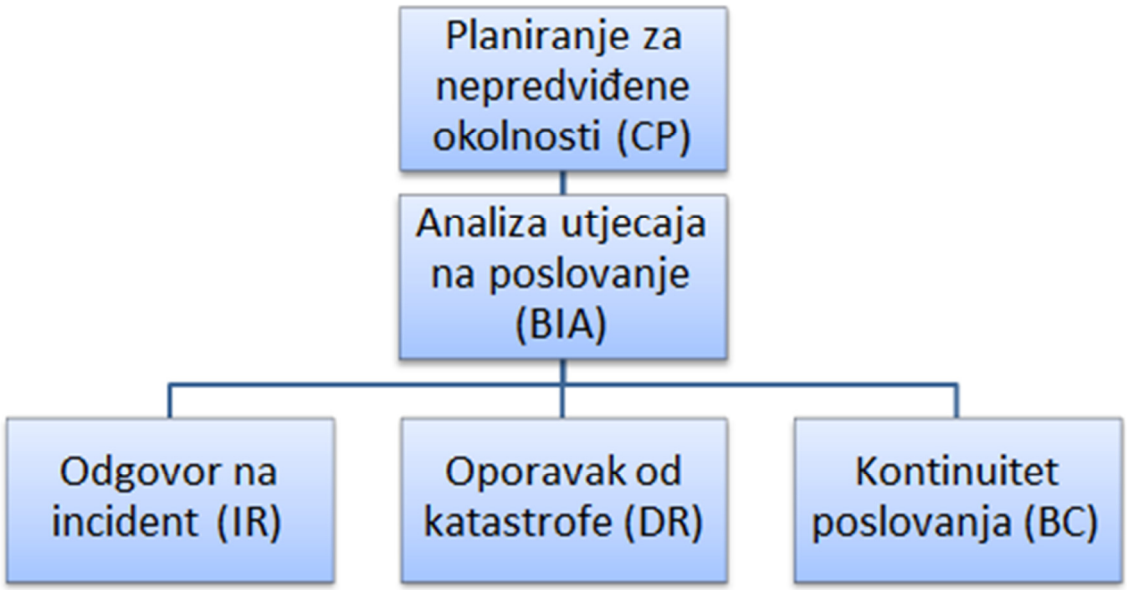
Organizacija može koristiti jedan ili više različitih pristupa odnosno strategija prilikom planiranja za nepredviđene okolnosti budući da oni nisu međusobno isključivi. Primjerice pristup **bunker** podrazumijeva smanjivanje rizika na razinu na kojoj su potrebni samo ograničeni planovi oporavka od katastrofe. Suprotno od toga, pristup **kontinuirane obrade** uključuje preslikavanje (engl. mirroring) poslovanja na alternativnu lokaciju. U slučaju katastrofe na primarnoj lokaciji, poslovanje se nastavlja na alternativnoj. U pristupu **distribuirane obrade** poslovanje se paralelno odvija na nekoliko različitih lokacija. U slučaju ispada jedne lokacije, poslovanje se, makar djelomično, nastavlja na drugim lokacijama. Proces planiranja za nepredviđene okolnosti može se **eksternalizirati** (engl. outsourcing), ali uz potporu specijalista koji su djelatnici organizacije [**4**].

2.1. Osnovni pojmovi

Opstanak svakog poslovanja ovisi o spremnosti za osiguranjem neprekidnosti osnovnih poslovnih aktivnosti i podupirućih servisa. Na strateškoj razini, uprava organizacije treba donijeti plan za nepredviđene okolnosti (engl. contingency planning, CP) za čiju izradu su odgovorni voditelji IT odjela i voditelj informacijske sigurnosti. Taj plan treba predviđati

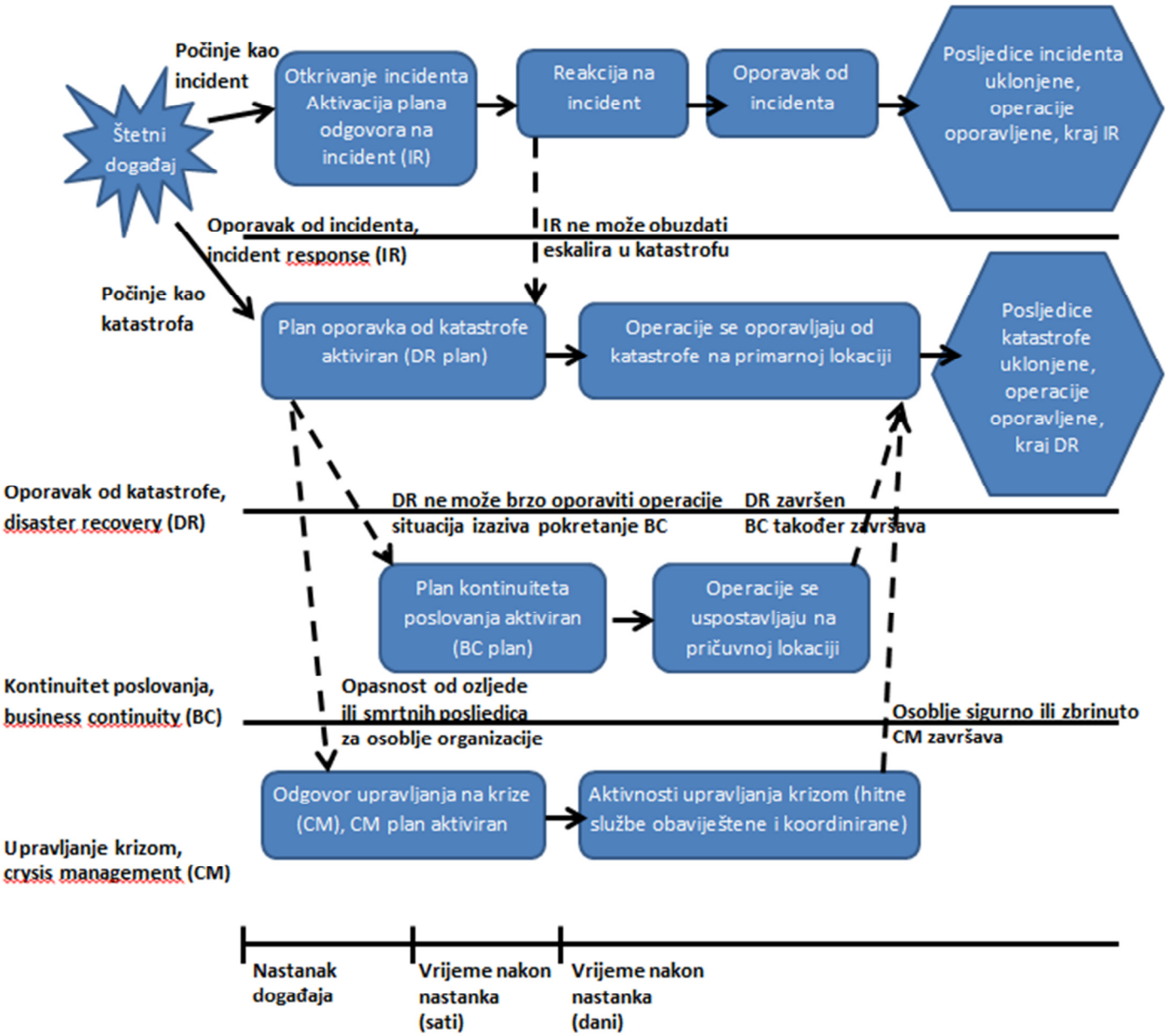
te davati smjernice za reakciju na te oporavak od svih štetnih događaja koji ugrožavaju sigurnost informacija i informacijske imovine organizacije. On pomaže da se organizacija vrati u normalan način poslovanja nakon nastanka neželjenog događaja.

Kako je prikazano na slici 2, CP obuhvaća planiranje odgovora na incident (engl. incident response, IR), planiranje oporavka od katastrofe (engl. disaster recovery, DR) i planiranje kontinuiteta poslovanja (engl. business continuity, BC), a temelji se na analizi utjecaja na poslovanje (engl. business impact analysis, BIA) koja je usko povezana s upravljanjem rizicima. [**5**].



Slika 2 – Komponente planiranja za nepredviđene okolnosti [5]

Prilikom nastanka štetnog događaja ovisno o razvoju situacije primijenit će se jedna ili više navedenih komponenti, počevši od najniže razine odgovora na incident (IR) do najviše razine upravljanja krizama (engl. crysis management, CM). Plan odgovora na incident predviđa trenutni odgovor na manje poteškoće koje utječu na poslovanje. Nakon toga, plan za oporavak od katastrofe usmjeren je na oporavak poslovnih sustava na glavnoj lokaciji nakon što se katastrofa dogodi. Plan kontinuiteta poslovanja provodi se usporedo s planom za oporavak od katastrofe u slučaju kada je štetni događaj velikih razmjera te nije moguće jednostavno oporaviti resurse. U pravilu podrazumijeva nastavak kritičnih poslovnih operacija na alternativnoj, pričuvnoj lokaciji [**5**]. Vremenska slika planiranja za nepredviđene slučajeve prikazana je na slici 3.

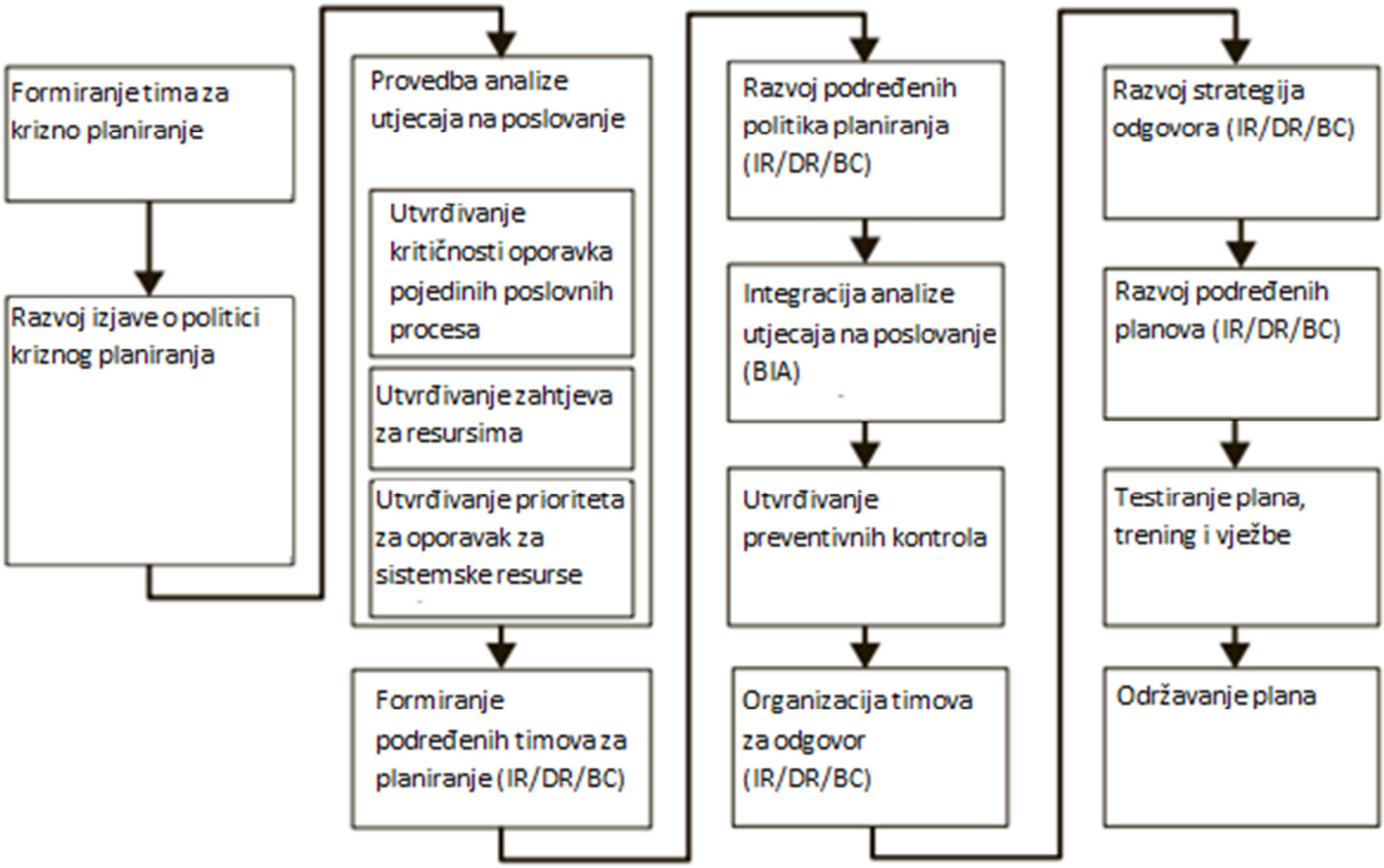


Slika 3 – Vremenska crta planiranja za nepredviđene slučajeve (CP) [5]

Kako je prikazano na slici 4, etape u provođenju planiranja za nepredviđene okolnosti su sljedeće [**6**] [**7**]:

1. Formiranje tima za krizno planiranje. Treba sadržavati predstavnike upravljačke razine, poslovnih procesa, te podređenih timova,

2. Razvoj izjave o politici kriznog planiranja. To je formalizirana politika temeljem koje će organizacija poslovati tijekom kriznih situacija te temeljem koje će djelovati podređeni timovi,
3. Provedba analize utjecaja na poslovanje. Tom analizom prepoznaju se poslovne funkcije i informacijski sustavi koji su kritični za cjelokupno poslovanje organizacije te se određuju njihovi prioriteti,
4. Formiranje podređenih timova za planiranje koji će razviti IR, DR i BC planove,
5. Razvoj podređenih politika planiranja za IR, DR i BC područje,
6. Integracija analize utjecaja na poslovanje (BIA) unutar svakog od navedenih podređenih područja kriznog planiranja. Svaki od podređenih timova treba procijeniti koji aspekt BIA analize najviše utječe na njihovo područje interesa te se usmjeriti na njega,
7. Utvrđivanje preventivnih kontrola što uključuje protumjere i zaštitne mjere kojima se nastoji umanjiti rizik nastanka te utjecaj nepredviđenih štetnih događaja na podatke, poslovne procese i osoblje organizacije,
8. Organizacija timova za odgovor sukladno kompetencijama i stručnim vještinama koje su potrebne za područje IR, DR i BC. Ovi timovi bit će izravno uključeni prilikom aktivacije plana odgovora na pojedini incident ili katastrofu,
9. Razvoj strategija odgovora koje će se primijeniti u slučaju događaja koji narušava poslovne operacije. Te strategije sadrže, primjerice, planove izrade pričuvnih kopija podataka, pohrane podataka na pričuvnu lokaciju i slično,
10. Razvoj podređenih planova koji za svako od područja (IR, DR, BC) opisuju aktivnosti koje je potrebno poduzeti kao odgovor na incident, oporavak od katastrofe ili nastavak poslovanja na pričuvnoj lokaciji,
11. Testiranje plana, trening i vježbe. Ovom aktivnosti provjerava se učinkovitost svakog od podređenih planova, a odgovorni djelatnici uvježbavaju njihovu provedbu,
12. Održavanje plana što podrazumijeva periodičku provjeru, procjenu plana te ažuriranje.



Slika 4 – Etape u provođenju planiranja za nepredviđene slučajeve [6] [7]

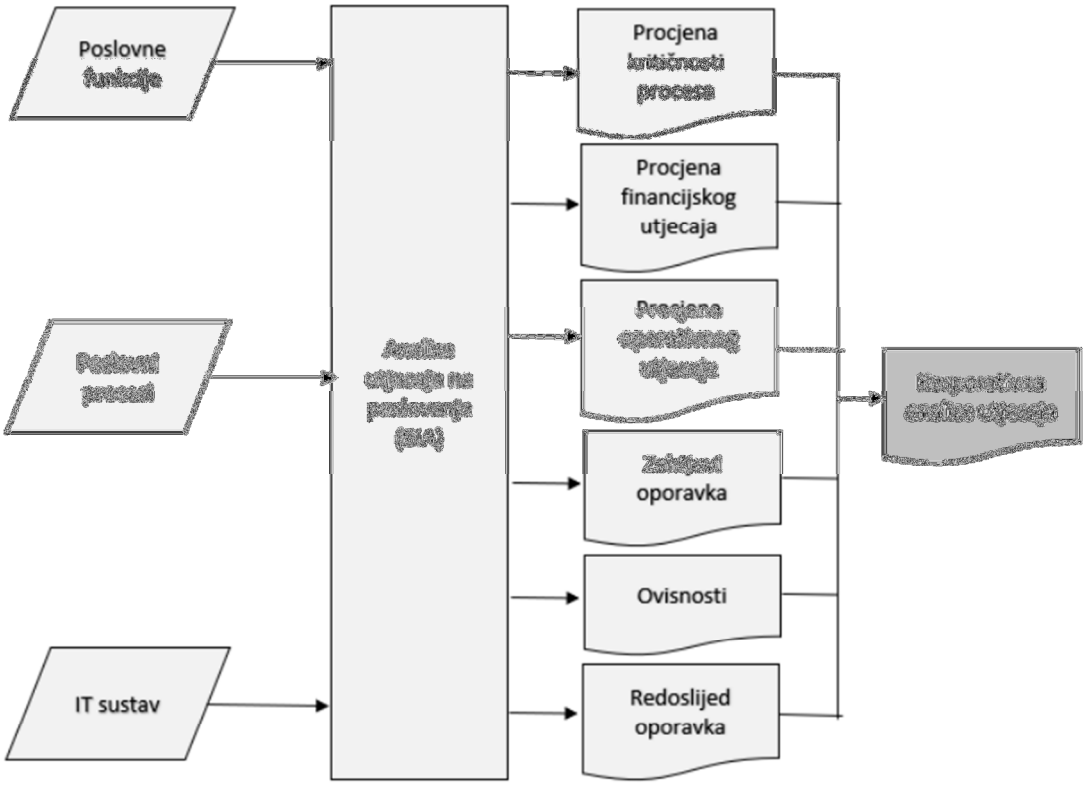
2.2. Analiza utjecaja na poslovanje

Analiza utjecaja na poslovanje (BIA) usmjerena je na kritične poslovne funkcije i utjecaj na poslovanje organizacije u slučaju da one nisu dostupne. BIA i upravljanje rizicima razlikuju se u perspektivi promatranja organizacije i njezinog poslovanja. Upravljanje rizicima razmatra prijetnje s kojima se organizacija susreće, a BIA je usmjerena na poslovne procese [**8**]. Nakon što organizacija izvrši kvalitetnu procjenu rizika te razradi proces upravljanja njima, može se posvetiti analizi utjecaja na poslovanje. Obje te sastavnice temelj su za izradu strategije planiranja za nepredviđene okolnosti.

Sa stajališta IT-a, cilj BIA-e je naći međuodnos između informacijskog sustava i kritičnih usluga koje on pruža te procijeniti učinke koji bi nastali u slučaju prekida funkcioniranja toga sustava [**6**]. Koraci u provedbi BIA-e prikazani na slici 5 su:

- Identifikacija ključnih poslovnih procesa i funkcija,
- Utvrđivanje međuovisnosti informacijskih sustava i poslovnih procesa,
- Utvrđivanje prioriteta i klasifikacija poslovnih procesa i funkcija,
- Utvrđivanje utjecaja prekida poslovnih procesa na sveukupne poslovne operacije, s naglaskom na financijske i operativne utjecaje,
- Utvrđivanje zahtijevanih vremena oporavka,
- Utvrđivanje preduvjeta za oporavak poslovanja,
- Utvrđivanje redoslijeda oporavka pojedinih procesa i funkcija.

Rezultat provedbe navedenih koraka je formalna, korporativna analiza utjecaja na poslovanje s kojom treba upoznati upravu organizacije.



Slika 5 – Koraci u provedbi BIA-e [**8**]

2.2.1. Identifikacija poslovnih procesa i funkcija

S obzirom na važnost za poslovanje organizacije, poslovne funkcije i procesi mogu se svrstati u **kritične**, **bitne**, **potrebne** i **poželjne** [**8**].

Kritične funkcije (engl. critical functions) su funkcije neophodne za poslovanje organizacije. S IT gledišta, prekid takve funkcije imat će vrlo ozbiljne sigurnosne, operativne i financijske učinke. Takav tim prekida može trajno onesposobiti organizaciju za obavljanje poslovanja. Informacijski sistemi vezani uz takve funkcije traže značajna ulaganja i trud da se osposobe za nastavak poslovanja koji često sami po sebi ometaju obavljanje nekih drugih poslovnih funkcija, ako ih je tada uopće moguće izvršavati. Prihvatljivo vrijeme oporavka u IT segmentu za takve funkcije mjeri se u satima, a ne u danima.

Bitne funkcije (engl. essential functions) su vrlo važne za poslovanje organizacije, ali ipak nisu ključne. Takva funkcija je, primjerice, isplata plaće zaposlenicima. Ona nije izravno vezana za poslovanje organizacije, ali bez nje organizacija ne može funkcionirati. Prihvatljivo vrijeme oporavka u IT segmentu za takve funkcije je maksimalno dan ili dva.

Potrebne funkcije (engl. necessary functions) su one čija nedostupnost ne će onemogućiti poslovanje organizacije odmah, ali njihova nedostupnost u duljem razdoblju može imati značajan učinak. S IT gledišta takve su funkcije, primjerice, email ili pristup Internetu odnosno sve funkcije koje se koriste u potpori poslovnim procesima. Prihvatljivo vrijeme oporavka za takve funkcije mjeri se u danima.

Poželjne funkcije (engl. desirable functions) imaju mali učinak na poslovanje organizacije. To su pomoćne funkcije koje su se razvile vremenom kao potpora poslovanju. U normalnim okolnostima, one se rutinski obavljaju i nemaju velik utjecaj. Veći prekid poslovanja, u stvari, predstavlja priliku za reviziju takvih funkcija. Ako se ispostavi da nisu uopće potrebne, ne će ih se ni vraćati. S IT gledišta, prihvatljivo vrijeme oporavka za takve funkcije mjeri se u tjednima, pa čak i mjesecima.

Poslovne funkcije svake organizacije mogu se svrstati u određene kategorije, primjerice, financijske, personalne, pravne, proizvodne, prodajne, skladišne, IT. Prilikom rada na BIA, za identifikaciju funkcija i procjenu njihove važnosti potrebna je suradnja osoba odgovornih za te poslovnih aktivnosti, primjerice, voditelja financija, voditelja informatike i ostalih. Rezultat ovog dijela BIA treba biti detaljan popis informacijskih sustava organiziran po funkcionalnim

područjima odnosno poslovnim funkcijama, načelan opis međuzavisnosti tih informacijskih sustava te okvirni troškovi u slučaju prekida tih funkcija. Podatci se prikupljaju intervjuima s voditeljima te uvidom u dokumentaciju.

2.2.2. Procjena utjecaja

Nakon identifikacije poslovnih funkcija i procesa, utvrđivanja njihove kritičnosti te međuodnosa s informacijskim sustavima, BIA prelazi na procjenu utjecaja nedostupnosti tih funkcija na poslovanje organizacije. Najvažniji utjecaji koji se moraju razmotriti u tom dijelu su financijski i operativni. Operativni podrazumijeva utjecaj prekida poslovanja na ljude, procese i tehnologiju, a financijski se odnosi na novčane efekte prekida poslovanja. Operativni utjecaji obuhvaćaju, primjerice, smanjivanje učinkovitosti rada zbog korištenja zaobilaznih procedura odrađivanja poslovnog procesa ili dodatno naprezanje radne snage u razdoblju oporavka poslovanja (prekovremeni rad). U smislu operativnih utjecaja, važno je razmotriti i moguće vanjske posljedice po organizaciju uzrokovane prekidom u poslovanju zbog nedostupnosti neke poslovne funkcije. Primjerice, ukoliko zbog prekida u poslovanju organizacija zakasni završiti poslovni projekt prema vanjskom naručitelju, on prema stavkama ugovora ima pravo tražiti isplatu odštete. Financijski učinci obuhvaćaju, primjerice, troškove nabavka uništene informatičke opreme izgubljene zbog požara u podatkovnom centru, troškove popravka zgrade, troškove za prekovremeni rad zaposlenih. Rezultat ovog dijela BIA je generalni popis utjecaja nedostupnosti poslovnih funkcija na poslovanje organizacije.

2.2.3. Zahtjevi oporavka

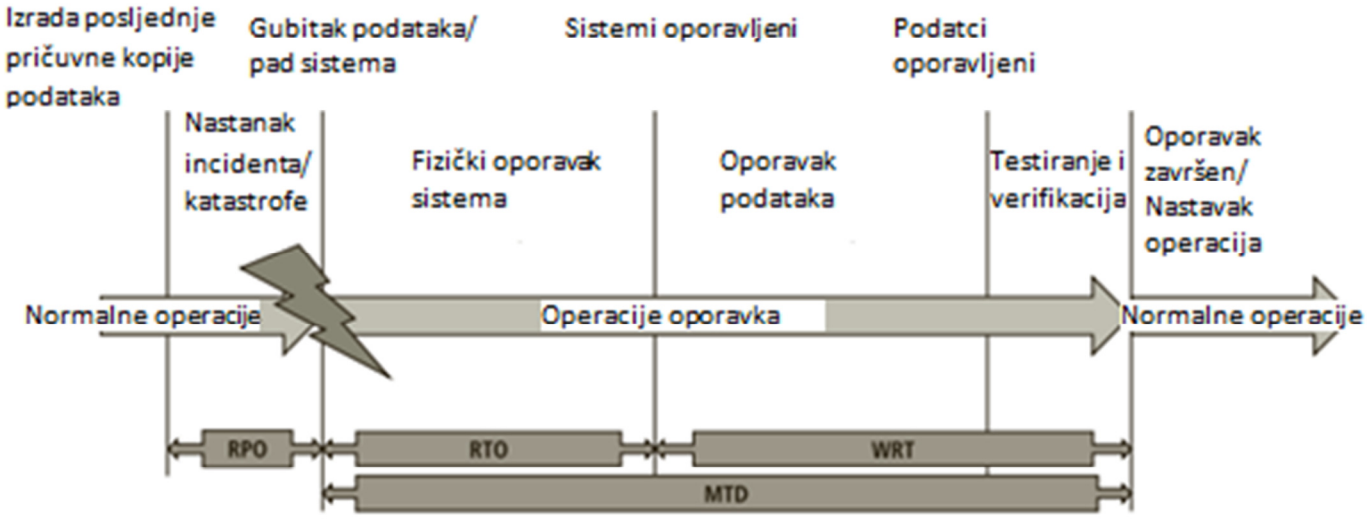
Zahtjevi vremena oporavka vezani su uz važnost funkcije za poslovanje organizacije. Postoji nekoliko pojmova koji su vezani uz taj segment BIA [**5**]:

1. Maksimalno prihvatljivo vrijeme ispada (engl. maximum tolerable downtime, MTD),
2. Ciljano vrijeme oporavka (engl. recovery time objective, RTO),
3. Vrijeme oporavka rada (engl. work recovery time, WRT),
4. Ciljana točka oporavka (engl. recovery point objective, RPO).

Maksimalno prihvatljivo vrijeme ispada sastoji se od vremena oporavka sustava (RTO) i vremena oporavka rada (WRT). Prema tome, **MTD = RTO + WRT**.

Ciljano vrijeme oporavka odnosi se na informacijski sustav. Ukoliko je poslovna funkcija bitna, njeno maksimalno prihvatljivo vrijeme ispada (MTD) je, primjerice, dva dana. U tom vremenu, sustavi moraju biti osposobljeni unutar jednog dana. Znači, RTO je jedan dan, a drugi dan je predviđen za uspostavu poslovanja (WRT). WRT je duži zato što osim što je informacijski sustav postao dostupan unutar RTO, potrebno je izvršiti njegovu sinkronizaciju s ostalim sustavima, vratiti podatke iz pričuvne kopije podataka (engl. backup), a podatke koje su ručno spremljeni prilikom prekida poslovanja treba ubaciti u sustav.

Ciljana točka oporavka predstavlja točku u poslovanju odnosno funkcioniranju sustava u koju se treba vratiti. Određeni gubitak podataka je neminovan, ali mora biti u prihvatljivoj razini. Primjerice, ukoliko se pričuvna kopija podataka izrađuje samo jednom tjedno, u nedjelju, a sustav se sruši u subotu, može doći do gubitka podataka od cijelog tog tjedna. U tom slučaju je RPO jedan tjedan. Ako je to previše, mora se unaprijediti procedura izrade pričuvnih kopija podataka.



Slika 6 – Vremenski okvir oporavka poslovanja [5]

Na slici 6 koja prikazuje vremenski okvir oporavka poslovanja RPO predstavlja maksimalno prihvatljiv gubitak podataka, a ovisi o tome kada je izrađena posljednja pričuvna kopija podataka. RTO je vrijeme potrebno za fizički oporavak informacijskog sustava. Vrijeme potrebno za oporavak podataka te njihovo testiranje i verifikaciju predstavlja WRT ili, drugim riječima, vrijeme oporavka rada. RTO i WRT zajedno čine MTD odnosno maksimalno

prihvatljivo vrijeme ispada. Po isteku MTD vremena organizacija se vraća u normalno poslovanje.

RTO kao vrijeme oporavka informacijskih sustava najizravnije je vezano s važnošću poslovne funkcije za organizaciju. Načelno, kritične funkcije imaju RTO od 0 do 12 sati, bitne od 13 do 24 sata, potrebne od 1 do 3 dana, a sporedne više od 3 dana. Kraći RTO donosi veće troškove. Primjerice, za obavljanje kritične poslovne funkcije koriste se SQL poslužitelji i aplikativni poslužitelj. U slučaju kvara poslužitelja, redovni odgovor od pružatelja usluge održavanja informacijskog sustava je 24 sata. Međutim, zbog važnosti ove funkcije s pružateljem usluga ugovoren je odgovor na kvar u roku 6 sati što se dodatno plaća svaki mjesec U ovom dijelu analize razradit će se zahtjevi za oporavak prema kategorijama poslovnih funkcija, od kritičnih do sporednih.

2.2.4. Međuovisnosti poslovnih funkcija

U nastavku analize potrebno je razmotriti međuodnos poslovnih funkcija, a osobito u relaciji prema informacijskim sustavima. Tako primjerice, s IT gledišta sustav A, interna elektronička pošta, je vrlo važan i voditelj IT odjela smatra da ga treba prvog osposobiti. Međutim, s gledišta sveukupnog poslovanja organizacije, sustav B, web aplikacija za prodaju, je najvažniji. Prema tome, sustav B ima prioritet za oporavak. Također, same poslovne funkcije organizacije međusobno su isprepletene i nedostupnost jedne može onemogućiti obavljanje i nekih drugih. Primjerice, financijske funkcije imaju utjecaj na cjelokupno poslovanje – od prodaje, marketinga, personalnog upravljanja do IT-a. Osim toga, u suvremenom poslovnom okruženju osobito značajan utjecaj ima IT. Nedostupnost IT funkcija odnosno ispad nekog od ključnih informacijskih sustava može ugroziti gotovo sve ostale poslovne funkcije organizacije.

Analiza međuovisnosti poslovnih funkcija te odnosa poslovnih funkcija s IT segmentom mora dati odgovor na mnoštvo pitanja, primjerice:

- Kako će prekid jedne određene poslovne funkcije utjecati na ostale i kada će to biti?
- Je li ta funkcija vezana za neke specifične resurse (određeni dobavljači, specijalna oprema)?
- Koje su ključne osobe za obavljanje te funkcije? Što će se dogoditi ako su te osobe nedostupne?

- Kako se ta funkcija obavlja – kontinuirano, povremeno, na dnevnoj ili tjednoj bazi? Postoji li neko kritično vrijeme kada je neophodna za poslovanje?
- Koji su IT resursi neophodni za obavljanje te funkcije?
- Postoje li neke ručne, zaobilazne procedure kojima se ona može izvršavati i ako informacijski sustav nije dostupan?

Nakon ovog dijela analize, a na temelju svih obrađenih sastavnica, pristupit će se izradi načelnog plana prioriteta redoslijeda oporavka. U njemu će funkcije biti razrađene ne samo po svojoj kritičnosti nego i po utjecaju na cjelokupno poslovanje te će jasno biti navedeno koje od njih se moraju prve osposobiti.

2.2.5. Izvješće o analizi utjecaja

Izvješće o analizi utjecaja na poslovanje treba dati na uvid voditeljima odjela odnosno osobama koje su sudjelovale u njegovoj izradi kako bi dali svoje komentare i mišljenja. Dorađena analiza nakon toga treba se prezentirati upravi. Ona će sadržavati mnoštvo podataka o poslovnim procesima i funkcijama, primjerice:

- Ključni procesi i funkcije,
- Međuovisnosti procesa i IT resursa,
- Kritičnost odnosno razina utjecaja na poslovanje,
- Ključne uloge i odgovornosti osoba zaduženih za njihovu provedbu,
- Zahtijevana vremena oporavka,
- Financijski, operativni, pravni, personalni učinci nedostupnosti,
- Ručne procedure za nastavak poslovanja u slučaju nedostupnosti.

Analiza predstavlja sveobuhvatan pregled poslovanja organizacije. U kombinaciji s procjenom odnosno upravljanjem rizicima temelj je izradu strategije upravljanja kontinuitetom poslovanja.

2.3. Upravljanje rizicima

Upravljanje kontinuitetom poslovanja u organizaciji usko je povezano s upravljanjem rizicima. A upravljanje rizicima u direktnoj je vezi s analizom utjecaja na poslovanje. Prema međunarodnoj normi ISO 31000 upravljanje rizikom predstavlja identifikaciju, procjenu i

određivanje prioriteta rizika nakon čega slijedi koordinirana i ekonomična primjena resursa za minimiziranje, praćenje i kontrolu vjerojatnosti ili učinka neočekivanih štetnih događaja na poslovanje organizacije. U ovoj normi se ističe kako upravljanje rizikom treba ugraditi u sve aspekte poslovanja, a ne promatrati ga kao zasebnu i samostalnu aktivnost. To je kontinuirani proces koji se bavi nesigurnostima u donošenju odluka i usmjeren je na krajnje rezultate. Osnovni pojmovi vezani uz rizike su kako slijedi [**9**]:

Rizik je djelovanje nesigurnosti na ciljeve organizacije koja može prouzročiti odstupanje od očekivanih rezultata. On je, u stvari, kalkulirana prognoza moguće štete odnosno gubitka.

Upravljanje rizikom u tom smislu je povećanje vjerojatnosti postizanja ciljeva, poboljšanje u utvrđivanju mogućnosti i opasnosti, uspostavljanje pouzdanog temelja za donošenje odluka i planiranje. Ono predstavlja također i svođenje gubitaka na najmanju mjeru te poboljšanje elastičnosti organizacije.

Kriterij rizika (engl. risk criteria) predstavlja referentnu točku koja može biti određeni standard, mjera ili očekivani cilj. Ta točka se koristi kako bi se procijenila razina odnosno utjecaj rizika na organizaciju.

Stav prema riziku (engl. risk attitude) definira poimanje i odnos prema rizicima unutar organizacije. Stav utječe na to hoće li se određeni rizici prihvatiti, kako će se raspodijeliti, umanjiti ili izbjeći.

Plan upravljanja rizikom (engl. risk management plan) opisuje načine na koje će organizacija upravljati rizicima. Plan određuje alate, pristup i količinu sredstava koji će se koristiti da bi se upravljalo rizicima. Plan upravljanja rizikom može se primijeniti na pojedine poslovne procese, projekte kao i na sveukupno poslovanje.

Nositelj rizika (engl. risk owner) je fizička ili pravna osoba koja je preuzela odgovornost upravljanjem rizika te je odgovorna i preuzima sve posljedice koje rizik donosi. To može biti cijela organizacija, ali češće se taj pojam odnosi na odgovornu cjelinu unutar organizacije, primjerice upravu.

Okvir upravljanja rizikom (engl. risk management framework) čine aspekti koji osiguravaju pretpostavke za projektiranje, primjenu, upravljanje, pregled i kontinuirano poboljšanje procesa upravljanja rizikom.

Vanjski utjecaji (engl. external context) su svi utjecaji izvan organizacije koji djeluju na njezino upravljanje rizikom i postizanje zadanih ciljeva, kao što su pravni, društveni, kulturalni, politički, ekonomski, tehnološki.

Unutarnji utjecaji (engl. internal context) su svi utjecaji unutar organizacije koji djeluju na njezino upravljanje rizikom i postizanje zadanih ciljeva. To mogu biti odnosi s dobavljačima, zaposlenici, kontrola kvalitete.

Identifikacija rizika (engl. risk identification) je aktivnost čiji je cilj pronalazak, prepoznavanje i opisivanje rizika koji mogu utjecati na organizaciju i njezino postizanje zadanih ciljeva. Koristi se kako bi se pronašli mogući izvori rizika te otkrile posljedice koje on nosi. Pri identifikacija rizika mogu se koristiti podatci dobiveni ispitivanjima i analizama, matematičke analize i savjeti stručnjaka.

Izvor rizika (engl. risk source) je točka odnosno događaj iz kojeg potječe rizik.

Razina rizika (engl. level of risk) je veličina rizika. Procjenjuje se kombinacijom posljedica i vjerojatnosti ostvarenja rizika. Razina rizika se može dodijeliti pojedinačnom riziku, kao i kombinaciji rizika.

Prijetnja je mogući uzrok neželjenog događaja. Taj događaj je uglavnom štetan za organizaciju i cilj je izbjeći ga. Svaka prijetnja sadrži izvor, motiv, učestalost ponavljanja, razornu moć i oblik.

Ranjivost je slabost unutar organizacije ili proizvodnog procesa koje je najmanje "otporno" na prijetnje. Ta slabost je najizgledniji izvor rizika u procesu. Ranjivost se uvijek promatra u vezi s prijetnjom.

Učinak je rezultat nekog djelovanja. On može biti pozitivan i negativan. Kombinacijom ranjivosti i određene prijetnje najčešće dobivamo negativne učinke koji donose štetu samom poslovnom procesu. Ta se šteta očituje u financijskim iznosima. Primjeri učinaka mogu biti gubitak profita, gubitak ugleda, gubitak podataka, gubitak tržišta.

$$\text{Rizik} = \text{Prijetnja} + (\text{Ranjivost} + \text{Vjerojatnost}) + \text{Učinak}$$ [**8**]

Rizik se može promatrati kao kombinacija prijetnje, specifične ranjivosti, vjerojatnosti da će se ta ranjivost iskoristiti te relativnog ili apsolutnog učinka koje će ona imati na organizaciju.

Tretman rizika (engl. risk treatment) je proces kojemu je cilj umanjiti razinu rizika kroz više koraka upotrebom različitih alata. Odgovornost za upotrebu najprihvatljivijeg tretmana rizika

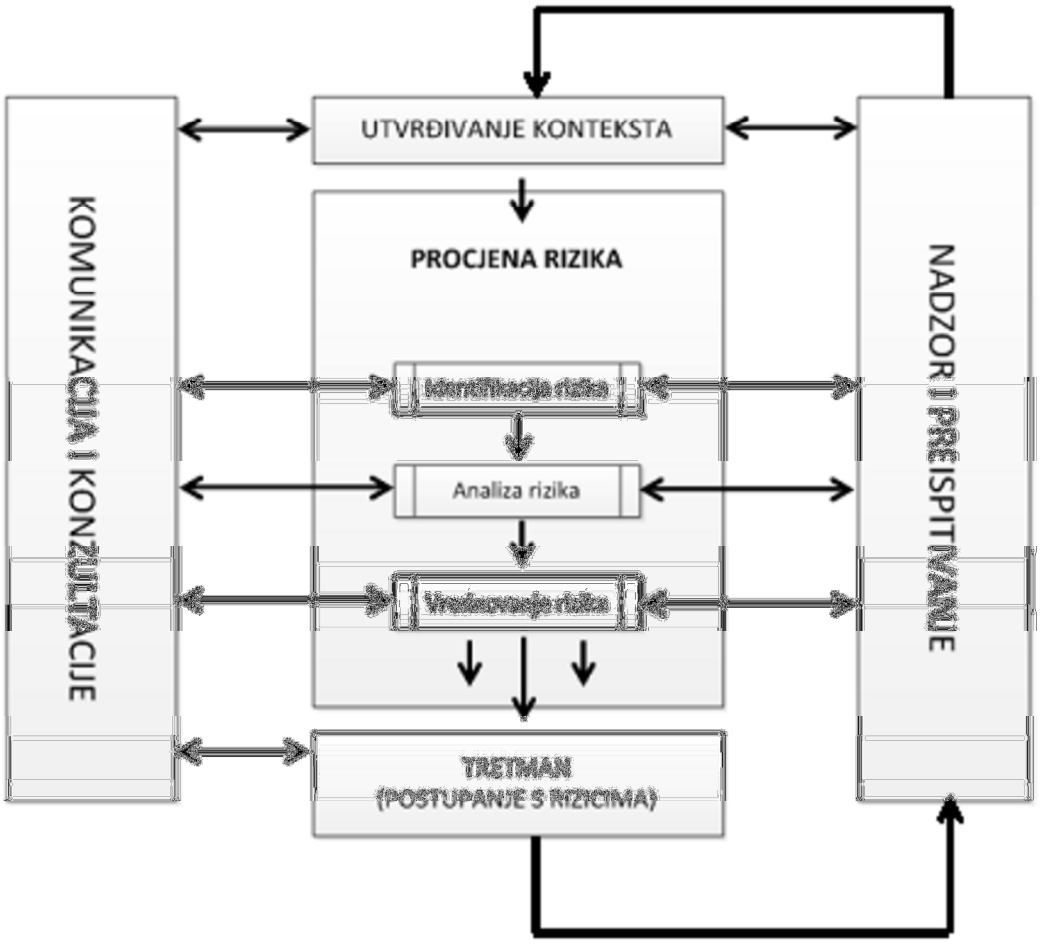
preuzima uprava organizacije. Osnovne metode koje se mogu koristiti pri tretiranju rizika su **izbjegavanje, smanjivanje, prihvaćanje** i **prenošenje.**

Rezidualni rizik (engl. residual risk) je rizik koji organizacija svjesno preuzima. Rezidualni rizik je posljedica nemogućnosti potpune eliminacije rizika. Kako bi rizik bio svjesno preuzet, mora biti u potpunosti poznat te smanjen na prihvatljivu razinu.

Vjerojatnost brojčano pokazuje kolika je šansa da se rizični događaj ostvari, a iskazuje se u rasponu od 0 (ne događa se) do 1 (sigurno će se dogoditi).

2.3.1. Proces upravljanja rizikom

Proces upravljanja rizikom prikazan na slici 7 trebao bi biti sastavni dio vođenja poslovanja, ugrađen u poslovanje te prilagođen vrsti posla kojom se organizacija bavi, a može se prikazati sljedećim dijagramom [**9**]:



Slika 7 – Proces upravljanja rizicima prema standardu ISO 31000 [9**]**

Komunikacija i konzultacije

Planovi za komunikaciju i konzultacije moraju se razviti u ranim fazama implementacije upravljanja rizikom. Komunikacija se mora odnositi na probleme koji se vežu uz same rizike, njihove uzroke, posljedice te načine da se ti rizici otklone. Efikasnom vanjskom i unutarnjom komunikacijom postiže se da su odgovorni za provođenje politike upravljanja rizicima u stalnom kontaktu s upravom organizacije. Na taj način sve važne informacije vezane uz rizike prenose se upravi i pomažu im za donošenje odluka u poslovanju. Time se postiže da su osobe koje donose odluke upoznate s rizicima koje one za sobom povlače.

Pristup upravljanju rizicima pri kojem se održava kvalitetna komunikacija pomaže u pravovremenom prepoznavanju rizika i njegovoj identifikaciji te olakšava sagledavanje rizika s različitih aspekata.

Utvrđivanje konteksta

Kroz ovu aktivnost organizacija određuje svoje ciljeve, definira vanjske i unutarnje parametre prema kojima se utvrđuje razina rizika te si određuje prihvatljivu razinu rizika.

Prilikom procjene vanjskog konteksta analiziraju se vanjski utjecaji na organizaciju poput stanja u gospodarstvu države i pravne regulative.

Unutarnji kontekst predstavlja stanje unutar organizacije. Budući da je upravljanje rizicima proces koji se provodi unutar organizacije, on mora biti usklađen s njezinim ciljevima odnosno cjelokupnim poslovanjem. Unutarnji kontekst obuhvaća vodstvo i organizacijsku strukturu,
politiku i ciljeve organizacije, strategiju poslovanja organizacije, odnose unutar organizacije te standarde po kojima organizacija posluje.

Što se tiče konteksta upravljanja rizikom, potrebno je utvrditi ciljeve, strategije i parametre organizacije unutar kojih će se provoditi proces upravljanja rizikom. Trebaju se definirati svi troškovi i resursi koji će biti potrebni za provođenje toga procesa. Taj kontekst obuhvaća definiranje ciljeva procesa upravljanja rizikom, definiranje odgovornosti unutar procesa upravljanja rizikom, definiranje raspona aktivnosti upravljanja rizikom, definiranje metoda procjene rizika te definiranje načina na koji će se izraziti uspješnost izvršenih procesa.

Procjena rizika

Procjena rizika sama po sebi prvi je korak u razradi strategije upravljanja kontinuitetom poslovanja. Plan kontinuiteta poslovanja kao rezultat te strategije mora se temeljiti na rizicima s kojima se organizacija susreće. Postoji mnoštvo nepovoljnih događaja koji predstavljaju rizik koji može prekinuti poslovanje. Zbog toga treba procijeniti koji su rizici najvjerojatniji i usmjeriti se na njih. Procjena rizika utječe na cjelokupno poslovanje organizacije, a osobito na informacijski sustav, njegovu arhitekturu, sigurnosna rješenja te sučelja prema ostalim poslovnim funkcijama.

Ovaj proces uključuje identifikaciju, analizu i vrednovanje rizika. U njemu se može koristiti kvantitativna ili kvalitativna metoda.

Kvantitativna metoda koristi brojčane vrijednosti za posljedice i vjerojatnost uz korištenje podataka iz raznih izvora. Kvaliteta procjene ovisi o točnosti i potpunosti korištenih brojčanih vrijednosti i valjanosti primijenjenih modela. Posljedice se mogu procijeniti modeliranjem rezultata nekog događaja ili niza događaja te ekstrapolacijom iz eksperimentalnih studija ili podataka iz prošlosti, a izražavaju se najčešće s obzirom na financijski učinak.

U kvalitativnoj metodi se koristi tekst za opisivanje veličine potencijalnih posljedica i vjerojatnosti da će te posljedice nastati. Kvalitativna se procjena može koristiti kao početna aktivnost za identifikaciju rizika koji zahtijevaju detaljniju analizu. Također se koristi u situacijama gdje je takva vrsta analize primjerena za donošenje odluka ili gdje brojčani podatci ili resursi nisu odgovarajući za kvantitativnu procjenu. Kvalitativnu procjenu treba dopuniti stvarnim informacijama i podatcima gdje god je to moguće.

Identifikacija rizika je aktivnost kojom se pronalaze izvori rizika. To mogu biti događaji u okolini organizacije, ali se mogu nalaziti i unutar organizacije. Osim mogućih izvora, potrebno je odrediti uzroke tih rizika, te procijeniti moguće posljedice. Cilj ovog koraka je izraditi popis rizika koji bi mogli imati utjecaj na organizaciju. Ti rizici mogu imati pozitivne i negativne utjecaje na organizaciju budući da mogu ubrzati, umanjiti, ugroziti ili olakšati ostvarenje ciljeva. Precizna identifikacija je vrlo važna, jer ako se pojedini rizik ne otkrije i ne identificira, on neće ulaziti u daljnje korake upravljanja rizikom. Ostvarenje negativnog rizika koji nije podvrgnut detaljnim operacijama upravljanja može imati iznimno loše posljedice na poslovanje organizacije. Identifikacija bi morala uključivati sve rizike neovisno o izvoru, odnosno je li on pod kontrolom organizacije ili nije, te je li on uopće poznat. Prilikom

identifikacije moraju se istražiti i izravne posljedice koje pojedini rizici nose. Vrlo je bitno da se u obzir uzme široka lepeza posljedica, kako bi se mogli izraditi planovi za sanaciju svih ostvarenih negativnih rizika. Zbog toga je važno da se prilikom identifikacije rizika uključe ljudi koji imaju u tome iskustva te da se primjene svi raspoloživi alati.

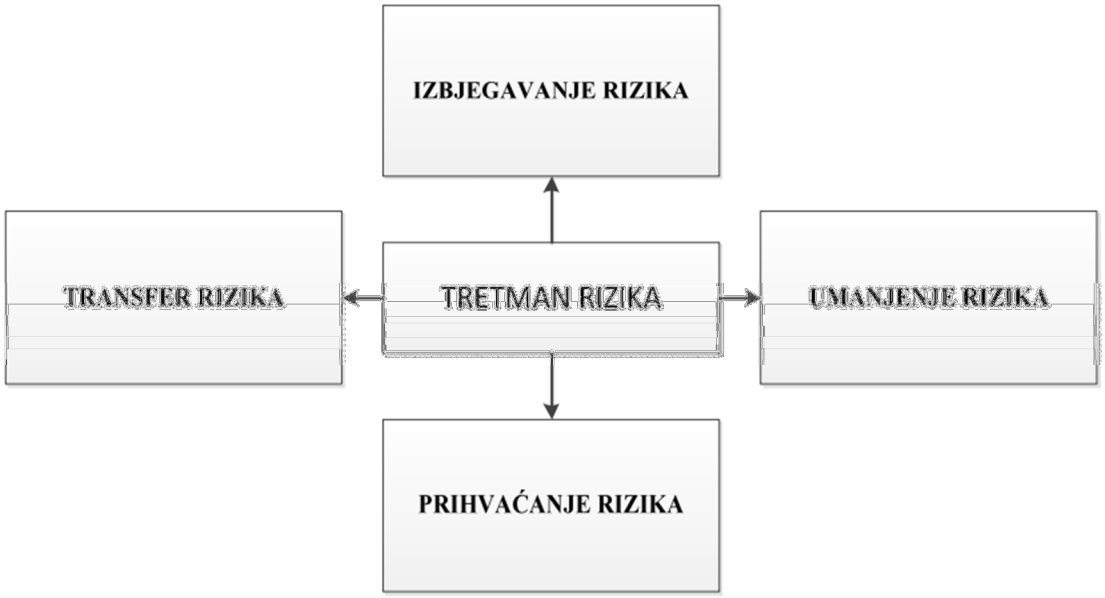
Analiza rizika slijedi nakon identifikacije. Tu se procjenjuje utjecaj rizika na organizaciju. Procjenjuje se vjerojatnosti njegova pojavljivanja te se mjeri veličina potencijalnog gubitka. Procjena zahtijeva određivanje nekih prioriteta. Određeni rizici, zbog većih potencijalnih gubitaka koje mogu uzrokovati, tražit će veću pozornost od drugih. Rizici se grupiraju u kategorije prema potencijalnim gubitcima. Svako izlaganje uz mogućnost gubitka koji bi predstavljao financijsku katastrofu stavlja se u isto kategoriju sa ostalim jednako opasnim izlaganjima. Ne postoji razlika između rizika u tom razredu. Mala je razlika ako je bankrot posljedica poplave, neosiguravanja od požara ili pada tržišta. Krajnji rezultat je isti. Zbog toga se rizici uobičajeno klasificiraju na opće grupe kao primjerice kritični, važni i nevažni. Kritični rizici su takvi u kojima su potencijalni gubici totalnih razmjera te mogu izazvati bankrot i raspad organizacije. Važni rizici nose potencijalne gubitke značajnih razmjera te bi nanijeli veliku financijsku štetu organizaciji. Nevažni rizici nose manje potencijalne gubitke koji mogu biti podmireni postojećim sredstvima ili prihodom organizacije. Kako bi se pojedini rizik mogao svrstati u jednu od ovih kategorija, mora se odrediti iznos financijskog gubitka kojeg on može prouzročiti te sposobnost organizacije da prihvati takav gubitak.

Ocjena rizika odnosi se odluke kojima se odabire alata za njegovo umanjenje. Kako bi rizik ocijenili koristimo podatke koje smo dobili analizom rizika. Ocjena rizika se sastoji od usporedbe analiziranog rizika s određenim kriterijima. Kriteriji se donose prije identifikacije rizika, a ako se zaključi da je rizik veći od prihvatljive razine, potrebno je poduzeti korake da se on umanji. Odluke se moraju bazirati na provjerenim podatcima i uzeti u obzir sve utjecaje koje donose. Uz to, bitno je osigurati da su sve odluke u skladu sa pravnim okvirom unutar i izvan organizacije. Ishodi ocjenjivanja mogu pokazati da je rizik prevelik i mora se umanjiti, da je prihvatljiv ili da se ne može procijeniti razina rizika te je potrebna detaljnija analiza.

Tretman rizika

Nakon identifikacije i procjene rizika treba razmotriti pristup koji će se koristiti pri upravljanju rizikom te odabir tehnike koja će se koristiti za svakog od njih. Drugim riječima,

tretman odnosno postupanje s rizikom prikazan na slici 8 predstavlja reakciju organizacije na njega.



Slika 8 – Tretman (postupanje) s rizicima prema standardu ISO 31000 [9]

Prikazane metode ne isključuju jedna drugu te se mogu kombinirati. **Izbjegavanje rizika** (engl. avoidance) je najjednostavniji oblik postupanja s rizikom. U tom slučaju organizacija jednostavno prestaje obavljati djelatnosti koje sa sobom vuku taj rizik. Na taj način organizacija se u potpunosti osigurala od gubitaka koje taj rizik može donijeti, ali se ta metoda rijetko može u potpunosti primijeniti. **Prijenos rizika** (engl. transfer) predstavlja aktivnost kojom se potencijalni gubitci od rizika prebacuju na nekog drugog izvan organizacije, tipično osiguravajuću kuću. Na taj način uobičajeno se prebacuju rizici vezani uz nekretnine u vlasništvu organizacije. **Smanjenje rizika** (engl. reduction) predstavlja mjeru u kojoj organizacija traži način da se umanje posljedice rizika koji se nikako ne mogu izbjeći. To se obično ostvaruje korištenjem određenih alata odnosno aktivnosti kojima se on nastoji umanjiti. Ukoliko se to ne uspije nakon prvog pokušaja, koristi se neki drugi alat ili se nastavlja s korištenjem istoga alata dok se rizik ne svede na prihvatljivu mjeru. **Prihvaćanje rizika** (engl. acceptance) provodi se na kraju, nakon što je potencijalni gubitak od rizika dovoljno smanjen.

Nadzor i preispitivanje

Sastavni dio procesa upravljanja rizikom predstavlja i nadzor te preispitivanje koje se odnosi na cjelokupan proces odnosno sve njegove korake. Nadzorom se poboljšava efikasnost provedbe procesa, provodi analiza cjelokupnog sustava upravljanja, pronalaze novi elementi bitni za njegov razvoj te identificiraju neki novi rizici. Rezultati nadzora i preispitivanja prezentiraju se pred osobama koje su odgovorne za upravljanje rizicima u organizaciji, a to je najčešće uprava.

2.3.2. Rizik informacijskog sustava

Rizik informacijskog sustava predstavlja vjerojatnost da određena prijetnja iskorištavanjem ranjivosti resursa informacijskog sustava (IS) ostvari negativan učinak na poslovanje organizacije [**10**]. Fokus procesa upravljanja rizicima IS je na informaciji, kao najvažnijem resursu IS. Informacijski sustav odnosno informacije koje on sadrži moraju sačuvati svojstva **povjerljivosti**, **integriteta** i **raspoloživosti** (engl. Confidentiality, Integrity, Availability, CIA) [**11**]**. Povjerljivost** je zaštita podataka od neovlaštenog pristupa. Osigurava se autentifikacijskim procedurama kao što su zaporke i liste kontrola pristupa. Gubitak povjerljivosti nastaje u slučaju neovlaštenog odnosno neplaniranog ili nenamjernog otkrivanja osjetljivih podataka. **Integritet** predstavlja zaštitu podataka od neovlaštene izmjene čime se osigurava da su oni točni i potpuni. Povreda integriteta može dovesti do prijevara ili pogrešnih odluka čime se narušava pravilno funkcioniranje informacijskog sustava. **Raspoloživost** podrazumijeva da su podatci i informacije koje se nalaze u informacijskom sustavu dostupne ovlaštenim korisnicima. Ona predstavlja jamstvo korisnicima da će im sustav biti na raspolaganju uvijek kada ga imaju potrebu koristiti. Štetni učinci rizika IS rezultiraju narušavanjem navedenih svojstava informacija, a proizlaze iz djelovanja prijetnji, koje štetne učinke ostvaruju iskorištavanjem ranjivosti resursa IS. Upravo zbog toga je bitno identificirati prijetnje i ranjivosti resursa IS te procijeniti rizike IS i njihove štetne učinke, prema kojima bi se postupalo primjenom odgovarajućih mjera.

Osnovni preduvjet za identifikaciju i procjenu rizika IS je poznavanje poslovnih ciljeva, poslovne strategije i poslovnih procesa organizacije, kako bi se mogao procijeniti realni utjecaj rizika IS na poslovanje. Nadalje, potrebno je identificirati sve resurse IS koji imaju ulogu u ostvarivanju poslovnih ciljeva i strategije te podrški poslovnim procesima, a potom i procijeniti njihovu važnost u tim ulogama. Osobito je važno spoznati i međusobne

ovisnosti resursa IS. Primjerice, ukoliko je neka informacija bitna za kritični poslovni proces, bitan će biti i poslužitelj baze podataka na kojem je ta informacija pohranjena, kao i operativni sustav i samo poslužiteljsko računalo, ali i mrežni uređaji i kablovi koji omogućuju dostupnost informacije putem osobnog računala krajnjem korisniku.

Rizici IS proizlaze iz djelovanja prijetnji. Prijetnje se obično dijele, s obzirom na mjesto nastanka, na unutrašnje i vanjske.

Unutrašnje prijetnje prvenstveno se odnose na ljudsko djelovanje od strane zaposlenika odnosno korisnika IS-a. Njihovo djelovanje, namjerno ili nenamjerno, može izložiti IS značajnim rizicima, primjerice [**8**]:

- neovlašteni pristup informacijama iznutra,
- greške u unosu podataka u aplikacije,
- nesvjesno odavanje povjerljivih informacija,
- greške u razvoju i održavanju IS,
- neprimjereno rukovanje informatičkom opremom.

Vanjske prijetnje mogu biti, primjerice [**8**]:

- maliciozni kod,
- socijalni inženjering,
- epidemije bolesti,
- prekid u napajanju električne mreže.

Identificirane prijetnje potrebno je staviti u kontekst ranjivosti resursa IS, koje pojedine prijetnje mogu iskoristiti te na taj način izazvati štetni učinak. Neke od ranjivosti mogu biti [**8**]:

- nepostojanje zaštite od malicioznog koda,
- pristup poslovnim aplikacijama nije kontroliran potvrdom identiteta korisnika,
- niska razinu svijesti o sigurnosti IS kod korisnika,
- nepostojanje sustava za besprekidnu opskrbu električnom energijom.

U konačnici, poznavanjem ranjivosti, prijetnji i njihovih štetnih učinaka na poslovanje mogu se procijeniti rizici IS, kroz dva njihova temeljna svojstva, a to je vjerojatnost da će prijetnja iskoristiti ranjivost resursa IS te razina štetnog učinka ukoliko prijetnja uspješno iskoristi ranjivost.

Odluka o načinu postupanja s rizicima IS u pravilu ovisi o samim rizicima te vrijednosti izloženih procesa i resursa. Kao što je i općenito slučaj s rizicima za poslovanje organizacije, prilikom upravljanja rizicima informacijskog sustava mogu se koristiti metode **izbjegavanja**, **smanjenja**, **transfera** i **prihvaćanja** [**8**].

Budući da se relativno mali broj rizika može izbjeći ili transferirati bez dodatnih ulaganja, organizacija nastoji rizike IS-a smanjiti kako bi se sveli na prihvatljivu razinu. U tom smislu, u raznim područjima upravljanja IS-om postoji cijeli raspon mjera i postupaka koje organizacija može poduzeti, a predstavljaju dobru praksu za smanjenje rizika IS-a [**10**].

Organizacija i upravljanje informacijskim sustavom

Funkcioniranje IS organizacije u znatnoj mjeri ovisi o podršci uprave subjekta. Uprava je odgovorna za organizaciju, strateško odlučivanje, dodjelu resursa i donošenje pravila i procedura u kontekstu upravljanja IS. U svrhu umanjenja rizika IS, preporučljivo je da uprava subjekta primijeni barem sljedeće mjere i postupke:

- Uspostava primjerene organizacijske strukture potrebne za funkcionalnost i sigurnost IS, sukladno poslovnim ciljevima subjekta,
- Osiguravanje resursa potrebnih za primjerenu funkcionalnost i sigurnost IS, poglavito u kontekstu stručnih kadrova, hardvera, softvera i podržavajuće infrastrukture,
- Imenovanje osobe odgovorne za upravljanje IT procesima i operacijama,
- Usklađivanje strategije razvoja IS i razvoja poslovne strategije subjekta,
- Razdvajanje funkcije upravljanja sigurnošću IS od drugih zaduženja vezanih uz IS. Sigurnosni i funkcionalni ciljevi IS mogu biti u suprotnosti u nekim situacijama, stoga je prisutna praksa razdvajanja tih funkcija dodjelom funkcija različitim osobama,
- Razdvajanje međusobno nesukladnih dužnosti u procesu upravljanja IT, kao primjerice sistemskog administratora od programera aplikacija, programera aplikacija od administratora baze podataka, sistemskog administratora od mrežnog administratora i drugo,
- Formiranje sustava unutarnjih kontrola IS u smislu funkcija unutarnje revizije, procjene rizika ili usklađenosti.

Razvoj i održavanje informacijskog sustava

Hardver, softver i podržavajuća infrastruktura zahtijevaju kontinuirano održavanje kako bi se osigurala njihova primjerena funkcionalnost. Neodržavana infrastruktura može biti

izložena različitim prijetnjama, kao što su primjerice greške u funkcioniranju operativnih sustava i aplikacija, kvarovi na računalima i mrežnoj opremi, kvarovi na podržavajućoj infrastrukturi, povećana izloženost djelovanju malicioznog koda i druge.

Kako bi se umanjili štetni učinci prijetnji nastalih zbog neprimjerenog održavanja IT, preporučljivo je:

- Osigurati primjereno održavanje hardvera, softvera i podržavajuće infrastrukture, u vidu nadogradnji i ispravljanja pogrešaka u softveru, redovnog servisiranja hardvera i podržavajuće infrastrukture, zamjene zastarjelih i dotrajalih komponenti i slično,
- Ograničiti ovlaštenja za izmjene na hardveru, softveru i podržavajućoj infrastrukturi isključivo na osobe koje su ovlaštene za to,
- Primjereno nadzirati ključne pokazatelje funkcionalnosti IT, kao što su primjerice slobodni kapaciteti medija za pohranu podataka, raspoloživost sistemskih resursa poslužiteljskih računala i slično.

Što se tiče aplikacija, kako bi se umanjili štetni učinci prijetnji nastalih zbog neprimjerenog pristupa njihovom razvoju, preporučljivo je:

- Uključiti krajnje korisnike aplikacija u proces izrade specifikacija aplikacije, kako bi se unaprijed definirale značajke poput korisničkog sučelja, ulaznih i izlaznih podataka i slično,
- Planirati sigurnosne kontrole u fazi razvoja, kao što su identifikacija korisnika i autorizacija pristupa resursima aplikacije, kriptografski mehanizmi, kontrole unosa podataka, kontrole izlaznih podataka i slično,
- Zaštititi izvorni kod aplikacija od neovlaštenog pristupa,
- Testirati funkcionalnost i sigurnost novih i izmijenjenih aplikacija prije njihovog uključenja u normalnu produkciju,
- Razdvojiti razvojno i testno okruženje aplikacija od produkcijskog, primjerice korištenjem odvojenih baza podataka ili potpuno odvojenih osobnih i poslužiteljskih računala za različita okruženja. Na taj način se znatno umanjuje rizik narušavanja cjelovitosti produkcijskih podataka tijekom razvoja ili testiranja,
- Izbjegavati koristiti produkcijske podatke za potrebe razvoja ili testiranja. Ukoliko se za potrebe razvoja ili testiranja koriste produkcijski podatci, povećava se rizik pristupa tim podatcima od strane neovlaštenih osoba. Stoga je preporučljivo takve

podatke ne koristiti prilikom razvoja ili testiranja ili pak prethodno iz njih ukloniti osjetljivi sadržaj poput osobnih podataka.

Upravljanje promjenama u informacijskom sustavu

Promjene u IS neizbježan su dio procesa razvoja i održavanja IS. Međutim, nekontrolirane promjene mogu proizvesti i negativne učinke, primjerice narušiti funkcionalnost komponenti IT, izložiti IS sigurnosnim prijetnjama ili donijeti probleme u radu korisnicima. Kako bi se umanjili štetni učinci prijetnji nastalih zbog nekontroliranih promjena, preporučljivo je osigurati da su odgovorne osobe za upravljanje IT upoznate s planiranim promjenama i potencijalnim rizicima tih promjena prije same provedbe, da su one odobrene od strane odgovorne osobe za upravljanje IT prije same provedbe, da su primjereno testirane prije njihove primjene u produkcijskim sustavima, a korisnici IS upoznati s promjenama ukoliko one utječu na provedbu korisničkih radnih zadataka.

Izdvajanje procesa informacijskog sustava

Izdvajanje procesa IS subjekata podrazumijeva uključivanje druge pravne ili fizičke osobe u obavljanje poslova vezanih uz IS, kao što su primjerice održavanje komponenti IT, razvoj aplikacija, izrada internetskih stranica, pružanje usluga uporabe tehničke i sigurnosne infrastrukture (smještaj internetskih stranica na poslužitelje pružatelja usluga), pružanje savjetodavnih usluga poput vođenja sigurnosti IS ili vođenja projekata i slično, pružanje usluga unutarnjih kontrola poput unutarnje revizije IS. Kupovina gotovog, tržišno dostupnog softvera za koji proizvođač izdaje ispravke i nadogradnje koje subjekt sam primjenjuje u svom sustavu ne smatra se izdvajanjem procesa. Međutim, u slučaju da proizvođač provodi primjenu ispravaka i nadogradnji u sustavu subjekta, što se smatra održavanjem sustava, odnosno da proizvođač provodi administraciju u vidu upravljanja korisničkim pravima i računima umjesto subjekta, što se smatra obradom podataka, govorimo o izdvajanju procesa. Izdvajanjem procesa organizacije ne mogu ujedno prebaciti i odgovornost za izvršavanje procesa i rezultirajuće posljedice na pružatelja usluge kojem je proces izdvojen. S obzirom na razinu ovisnosti poslovanja subjekta o izdvojenim procesima, može se procijeniti značajnost izdvajanja. Primjerice, ukoliko o nekom izdvajanju ovisi funkcioniranje središnjih poslovnih procesa, ili pak ukoliko se izdvojenim procesom obrađuju osjetljivi podatci poput financijskih ili osobnih, možemo govoriti o značajnom izdvajanju. Ovisno o značaju izdvajanja, subjekti se mogu izložiti različitim rizicima, od manjih neugodnosti do

znatnih financijskih gubitaka, narušavanja povjerljivosti, cjelovitosti i dostupnosti osjetljivih podataka te prekida središnjih poslovnih procesa, izazvanih djelovanjem prijetnji, kao što su primjerice:

- nemogućnost pružatelja da osigura primjerenu uslugu,
- potpuni prekid pružanja usluge, primjerice uslijed stečaja pružatelja, više sile i slično,
- krađu i oštećenje resursa IS od strane pružatelja,
- odavanje povjerljivih podataka od strane pružatelja,
- nemogućnost izvršavanja ugovornih obveza subjekta prema pružatelju.

Zbog svega navedenog, a u svrhu smanjivanja rizika vezanih uz vanjske pružatelje usluga organizacija treba dobro procijeniti rizike izdvajanja procesa vanjskom pružatelju, procijeniti primjerenost pružatelja usluga, definirati i sklopiti ugovor koji odgovara usluzi koja se traži te osigurati primjeren nadzor nad pružateljem usluge prilikom obavljanja posla.

Fizička sigurnost

Fizička sigurnost podrazumijeva primjenu mjera i postupaka kojima se kontrolira fizički pristup resursima IS. Ukoliko one ne postoje, organizacije se mogu izložiti rizicima otuđenja i oštećenja informatičke opreme te dodatno povećati rizike neovlaštenog pristupa osjetljivim podatcima pohranjenima na informatičkoj opremi. Kako bi se umanjili rizici koji proizlaze iz nepostojanja primjerenih kontrola fizičke sigurnosti, preporučljivo je:

- Smjestiti važnu informatičku opremu poput poslužiteljskih računala, medija za pohranu podataka, konfiguracijskih terminala, aktivne mrežne opreme u posebne prostorije,
- Omogućiti pravo pristupa prostorijama u kojima je smještena važna informatička oprema samo ovlaštenim osobama,
- Osigurati da su osobe koje pristupaju tim prostorijama, a koje za to inače nemaju pravo pristupa, pod stalnim nadzorom ovlaštenih osoba. To se prije svega odnosi na vanjske suradnike koje pristupaju prostorijama zbog održavanja informatičke opreme,
- Voditi evidenciju osoba koje pristupaju prostorijama s važnom informatičkom opremom, ručnim ili automatiziranim putem,
- Osigurati dodatne mjere za kontrolu pristupa u prostorije s važnom informatičkom opremom poput video nadzora, protuprovalnih vrata i alarma,

- Osigurati kontrolu pristupa medijima za pohranu podataka koji su bez nadzora, primjerice zaključavanjem u ormar ili sigurnosni sef papirnatih dokumenata, CD, DVD i USB podatkovnih medija, pametnih kartica i slično.

Važnu informatičku opremu potrebno je također zaštititi od rizika izazvanih djelovanjem okoliša poput curenja vode ili požara. Prostorije u kojima se nalaze obavezno moraju imati klima uređaje te sustave za detekciju i gašenje požara.

Logičke kontrole pristupa

Ovim kontrolama sprječavaju se rizici neovlaštenog pristupa podatcima unutar IS-a zaposlenicima, vanjskim suradnicima te svim drugim osobama koje imaju pristup na IS. Logičke kontrole moraju biti podešene na operativnim sustavima poslužiteljskih i korisničkih računala, na aktivnoj mrežnoj opremi te sistemskim i poslovnim aplikacijama IS-a. U okviru logičkih kontrola potrebno je regulirati politiku dodjele, izmjene i ukidanja korisničkih računa koristeći načelo minimalnih potrebnih prava za obavljanje radnih zadataka. Korisnički računi moraju biti jednoznačno vezani s korisnikom, primjerice *DOMENA\ime.prezime*, a svaki korisnik mora imati vlastiti račun. Administratori IS-a moraju voditi računa da su korisnički računi s proširenim ovlastima koje koriste za administraciju također vezani na pojedinu osobu. Vezano uz to, potrebno je razraditi i politiku zaporki s naglaskom na kompleksnost i vrijeme nakon kojega se mora zamijeniti. Osim toga, zaporke koje su na informatičkoj opremi inicijalno postavljene od strane proizvođača administratori trebaju izmijeniti i postaviti kompleksne.

Sigurnost računalnih mreža

U većini slučajeva lokalnim mrežama se vrši najveći dio prijenosa osjetljivih poslovnih podataka te je njima potrebno pružiti i najveću pozornost u kontekstu zaštite i sigurnosti. Neprimjereno zaštićene računalne mreže izložene su rizicima neovlaštenog pristupa i zlouporabe što može dovesti do narušavanja povjerljivosti, cjelovitosti i dostupnosti važnih poslovnih informacija. Kako bi se umanjili rizici proizašli iz neprimjerene zaštite računalnih mreža preporučljivo je:

- Ograničiti pristup konfiguracijskim sučeljima mrežnih uređaja, poput preklopnika i usmjerivača, na isključivo za to ovlaštene osobe,

- Primjereno zaštititi računala i poslužiteljske servise subjekta kojima je omogućen pristup putem javnih mreža vatrozidom ili sustavom za detekciju neovlaštenog pristupa,
- Računala i poslužiteljske servise kojima je omogućen pristup putem javnih mreža izdvojiti u mrežni segment odvojen od lokalne računalne mreže,
- Primjereno zaštititi prijenos osjetljivih podataka putem javnih mreža, primjerice kriptografskom zaštitom SSL/TLS komunikacijskog protokola.

Ukoliko je za djelatnike organizacije omogućen udaljeni pristup na IS, prijenos podataka mora biti zaštićen sigurnosnim protokolima poput SSL ili IPSEC te se treba uspostaviti vođenje zapisa o aktivnostima udaljenog korisnika.

Sigurnost prijenosnih uređaja i medija za pohranu podataka

Prijenosni uređaji i mediji za pohranu podataka, poput prijenosnih računala, pametnih telefona i CD/DVD/USB medija za pohranu podataka izloženi su povećanim rizicima otuđenja i gubitka zbog svoje prenosivosti, a time i neovlaštenom pristupu osjetljivim podatcima ukoliko su takvi na njima pohranjeni. Kako bi se umanjili rizici koji proizlaze iz gubitka ili otuđenja opreme dobre su prakse koristiti tehnike kriptiranja povjerljivih podataka pohranjenih na njima, zaštititi pristup sučeljima operativnih sustava metodama potvrde identiteta korisnika putem PIN-a ili skeniranjem otiska prsta te omogućiti udaljeno brisanje podataka pohranjenih na pametnim telefonima u slučajevima njihovog gubitka ili otuđenja.

Upravljanje operativnim i sistemskim zapisima

Operativni i sistemski zapisi komponenti IS-a, primjerice aplikacija i operativnih sustava računala, generiraju se u svrhu bilježenja informacija o aktivnostima provedenim na njima. U slučaju incidenta, operativni i sistemski zapisi imaju ključnu ulogu u rekonstrukciji događaja i utvrđivanju eventualne odgovornosti korisnika. U cilju primjerenog upravljanja operativnim i sistemskim zapisima preporučljivo je:

- Osigurati generiranje operativnih i sistemskih zapisa u svim važnim komponentama IS-a u mjeri dovoljnoj za rekonstrukciju događaja i utvrđivanje individualne odgovornosti korisnika. Korisničko ime osobe koja je provela aktivnost, opis aktivnosti, naziv komponente IS i vrijeme događaja minimalni su podatci koji bi trebali biti prisutni u većini zapisa,

- Zaštititi operativne i sistemske zapise važnih komponenti IS-a od neovlaštenog pristupa,
- Izrađivati pričuvne kopije (engl. backup) operativnih i sistemskih zapisa važnih komponenti IS-a,
- Osigurati točnost mjerenja vremena u komponentama IS-a koje generiraju operativne i sistemske zapise kako bi se osigurala točnost podataka o vremenu nastanka događaja.

Zaštita od malicioznog koda

Suvremeni maliciozni kod može prouzročiti različite štetne učinke na IS-a. Dobar primjer za to je ucjenjivački softver (engl. ransomware) koji može onemogućiti pristup sve podatke organizacije ukoliko se proširi na poslužitelje. Zbog toga na korisničkim računalima i poslužiteljima u IS-u mora biti instaliran kvalitetan antivirusni softver koji se redovito ažurira. Također se trebaju instalirati sigurnosne zakrpe na operativnim sustavima. Pristup na internetske stranice s korisničkih računala treba biti omogućen isključivo kroz korištenje posredničkog (engl. Proxy) poslužitelja koji svojim sigurnosnim mehanizmima otežava pristup malicioznog koda sa zaraženih internetskih stranica. Softver koji radi antivirusnu provjeru privitaka elektroničke pošte također je koristan alat za smanjenje rizika od malicioznog koda.

2.4. Odgovor na incident

Neplanirani događaji koji se mogu okarakterizirati kao incidenti su takvi koji mogu nanijeti štetu informacijskoj imovini organizacije te ugroziti povjerljivost, integritet i raspoloživost (CIA) informacijskih resursa. Ovo područje planiranja za nepredviđene okolnosti u pravilu se fokusira na štetne događaje u IT segmentu poslovanja organizacije. Izradom plana odgovora na incident bavi se tim za IR, a za provedbu je zadužen tim za odgovor na računalne sigurnosne incidente (engl. Computer Security Incident Response Team, CSIRT). Prema tome, na incidente se odgovara kada se dogode (reaktivno) te nema mnogo proaktivnog djelovanja kako bi se izbjeglo da se isti uopće dogode [**5**].

Aktivnosti odgovora na incident sastoje se od faze planiranja, otkrivanja, reakcije i oporavka. Faza planiranja temelji se na BIA. U njoj se razvijaju scenariji ili predefinirani odgovori koje će CSIRT te djelatnici koji se bave informacijskom sigurnošću odraditi u trenutku nastanka incidenta određene vrste. To omogućuje organizaciji da brzo i učinkovito reagira na pojavu

incidenta. Planovi koji se izrađuju u ovoj fazi moraju se periodički testirati kako bi se utvrdilo odgovaraju li situacijama koje se mogu stvarno dogoditi te se mora uvježbavati njihova provedba. Faza otkrivanja obuhvaća sve situacije kada netko prijavi neobičnu pojavu. To može biti bilo koji djelatnik organizacije koji je korisnik informacijskog sustava i koji obavještava sistemskog, sigurnosnog administratora ili nadređenog kako je uočio tehnički problem na informacijskom sustavu, od sporog rada, nedostupnosti nekih datoteka na poslužitelju do rušenja sistema prilikom rada. Osim prijave od strane korisnika sustava incident može prijaviti i specijalizirani softver za otkrivanje upada (engl. intrusion detection system, IDS), antivirusni softver, a može ga otkriti i administrator sustava. U ovoj fazi važno je razlučiti je li štetni događaj nastao zbog softverske ili hardverske greške, zagušenog mrežnog prometa, problema kod pružatelja usluga ili je stvarno riječ o napadu na informacijsku imovinu organizacije. Jedino se posljednje navedeni tip događaja može okarakterizirati kao incident. Kada se događaj klasificira kao incident, voditelj sigurnosti ili druga osoba odgovorna za sigurnost treba odlučiti hoće li se primijeniti plan odgovora na incident i koji točno.

U svakom slučaju, prilikom nastanka incidenta mora se obavijestiti osoblje koje je ključno za njegovo rješavanje, u pravilu CSIRT. Prvi koraci usmjereni su na zaustavljanje incidenta ili ograničavanje njegovog štetnog utjecaja. Nakon toga poduzimaju se mjere oporavka podataka, sustava i/ili procesa oštećenih incidentom. Pri tome je važno provesti kvalitetnu procjenu nastale štete kako se ne bi dogodilo da se nešto zaboravi popraviti. Na kraju se incident treba dokumentirati na način da se zabilježi što se dogodilo, kada i gdje, zašto se to dogodilo, tko je sudjelovao u njegovom nastanku te kako je riješen. Dokumentiranjem se radi temelj za kvalitetnije postupanje u slučaju sličnog incidenta u budućnosti [**5**].

2.5. Oporavak od katastrofe

Upravljanje kontinuitetom poslovanja u IT segmentu usko je povezano s oporavkom od katastrofe (DR). DR je dio kontinuiteta poslovanja koji se bavi neposrednim utjecajem nakon nastanka neželjenog događaja. Može se definirati kao proces, politike i procedure povezane s pripremom aktivnosti u svrhu kontinuiteta poslovanja nakon što se dogodi neželjeni događaj odnosno katastrofa [**12**]. Katastrofa je neželjeni i neočekivani štetni događaj koji organizaciji

onemogućuje obavljanje kritičnih poslovnih funkcija kroz neodređeni vremenski period i rezultira velikom štetom (ne samo financijskom) za njezino poslovanje. To može biti [**8**]:

- nedostupnost glavne lokacije organizacije zbog prirodne katastrofe ili požara,
- nedostupnost IT infrastrukture na glavnoj lokaciji zbog kvara hardvera ili softvera većih razmjera,
- nedostupnost ključnih djelatnika organizacije zbog epidemije,
- dugotrajni prekid isporuke električne energije,
- prekid ključnih usluga dobavljača.

Planiranjem oporavka od katastrofe definiraju se aktivnosti koje je potrebno poduzeti za ponovno uspostavljanje poslovnih procesa nakon prekida uzrokovanog neočekivanim štetnim događajem. Njime se želi postići da djelatnici organizacije koji sudjeluju u oporavku točno znaju koje aktivnosti trebaju poduzeti, na koji način te kojim redoslijedom. To se postiže dokumentiranjem i redovitim testiranjem procedura jer se ne može čekati da se katastrofa stvarno dogodi kako bi se provjerilo hoće li plan raditi u praksi.

2.5.1. Faze u planiranju oporavka od katastrofe

Kada se govori o oporavku od katastrofe u IT području, prva asocijacija je izrada pričuvne kopije podataka. Pričuvna kopija podataka predstavlja važnu komponentu za oporavak od katastrofe odnosno što skoriji nastavak poslovanja, ali sama po sebi nije dovoljna. Oporavak od katastrofe obuhvaća procedure kojim se informatički servisi i infrastruktura vraćaju u operativno stanje kako bi se moglo nastaviti poslovanje organizacije. Postoje različite definicije oporavka od katastrofe, no svaki plan oporavka mora sadržavati sljedeće [**8**]:

1. popis IT sredstava – inventura hardvera, sustava i aplikacija koje se koriste u organizaciji,
2. procjenu rizika – treba ju izraditi za svaki ključni informacijski sustav; predvidjeti vjerojatnost nastanka neočekivanog štetnog događaja (katastrofe) te štetu može nastati,
3. klasifikaciju važnosti – pojedini informacijski sustavi, hardver, infrastruktura važniji su za poslovanje od drugih; neki su kritični odnosno bez njih poslovanje stoji, a drugi mogu biti osposobljeni u kasnijoj fazi,
4. RTO i RPO,

5. popis aktivnosti – procedure kojima se uspostavlja nastavak poslovanja organizacije u slučaju katastrofe; kratkoročnima se uspostavljaju osnovne funkcionalnosti, dugoročnima se poslovanje vraća u uobičajeno stanje; osim automatiziranih procedura za oporavak informacijskog sustava koje se izvršavaju neovisno o čovjeku, a moraju biti ovdje dokumentirane, u tom dijelu plana navedene su i precizne instrukcije za sve djelatnike koji sudjeluju u oporavku odnosno tu piše tko mora što odraditi.

Aktivnosti oporavka uključuju najmanje sljedeće [**12**]:

1. oporavak hardvera – u slučaju kvara ili oštećenja produkcijskog hardvera podrazumijeva osposobljavanje zamjenskih hardverskih komponenti na glavnoj odnosno pričuvnoj lokaciji; provedbom ove aktivnosti moraju se osposobiti poslužitelji, mrežna oprema, vatrozid te sustav za prevenciju upada (engl. Intrusion Prevention System, IPS);
2. oporavak operativnih sustava – operativni sustavi i podatkovni sustavi mogu se pohraniti na posebne poslužitelje, mrežne instalacijske upravitelje (engl. Network Installation Manager, NIM) odakle se mogu povući u slučaju katastrofe; glavni servisi koji se trebaju što ranije osposobiti su DNS (engl. Domain Name System) koji služi za pronalazak poslužitelja i servisa prema nazivu te Active Directory koji služi za upravljanje računalnim i mrežnim resursima – računalima, datotekama, korisnicima i grupama korisnika; upute za instalaciju i konfiguraciju operativnih sustava u slučaju katastrofe potrebno je unaprijed pripremiti;
3. oporavak baza podataka i arhivskih zapisa – procedure povratka baza podataka iz pričuvnih kopija podataka također trebaju biti unaprijed definirane;
4. oporavak spremišta podataka (engl. Storage Area Network SAN) – pričuvni hardver (uređaji za pohranu podataka, diskovi) trebaju biti spremni za slučaj katastrofe, procedure za selidbu produkcijskih podataka na njih trebaju biti unaprijed definirane;
5. oporavak aplikacija – uključuje povratak aplikacijskih podataka, sinkroniziranje s podatcima na pričuvnoj lokaciji te provjeru jesu li oporavljeni ispravni i najnoviji podatci;
6. testiranje procedura oporavka – od jednostavnih testova po kontrolnoj listi, preko strukturiranih etapnih testova do simulacijskih testova i realnih testova s prekidima; cilj testiranja je provjeriti učinkovitost plana u realnim uvjetima te ga revidirati kako bi se utvrdilo je li u skladu s politikama i ciljevima poslovanja organizacije.

Prema tome, plan oporavka od katastrofe u IT području treba identificirati i klasificirati rizike i prijetnje koji mogu dovesti do katastrofe, definirati resurse i procese koji će osigurati neprekidnost poslovanja tokom samog događanja katastrofe te odrediti mehanizme ponovnog uspostavljanja normalnog rada informacijskog sustava i poslovanja, nakon što su ublažene posljedice katastrofe. Potencijalne katastrofe uključuju kvarove na aplikacijama, virtualnim poslužiteljima, fizičkim poslužiteljima, mrežnim vezama, podatkovnim centrima, incidente na cijelom objektu poput požara te prirodne katastrofe poput potresa ili poplave. U njemu moraju biti imenovane konkretne osobe koje su za zadužene za njegovo izvršenje i unaprjeđenje. Mora se periodički testirati, evaluirati i dorađivati, osobito zato što se IT infrastruktura (hardver i sustavi) kontinuirano nadograđuje i zamjenjuje novijom.

2.5.2. Strategije oporavka od katastrofe

Odabir strategije oporavka vrši se na temelju više kriterija od kojih su najvažniji najduže RTO, RPO, minimalna prihvatljiva razina usluge te cijena implementacije. U načelu, prihvatljive su one strategije koje omogućuju oporavak od katastrofe i nastavak poslovanja u vremenu jednakom ili manjem od utvrđenog RTO-a, a čiji trošak ne prelazi maksimalni iznos troška koji je organizacija odlučila tolerirati u slučaju neočekivanog štetnog događaja. Strategija oporavka od katastrofe obuhvaća sve resurse koji su potrebni za poslovanje [**13**]:

- osoblje,
- uredski prostor,
- IT oprema i sustavi,
- podatci,
- usluge i dobavljači,
- transport.

Oporavak od katastrofe u IT području zasniva se na redundantnosti lokacije i/ili IT opreme te replikaciji podataka i stanja aplikacija. Odabir konkretnog plana oporavka ovisi o konkretnim potrebama poslovanja organizacije te financijskim sredstvima s kojima raspolaže [**14**].

Najjednostavniji plan je **fokusiran na pričuvnu kopiju podataka.** Njega primjenjuju organizacije koje nemaju sredstava ili potrebu za sveobuhvatnim planom oporavka. Te organizacije najčešće koriste vanjsku uslugu (oblak) na koju pohranjuju podatke s produkcijskog informacijskog sustava. U slučaju katastrofe podatci su zaštićeni i mogu se

vratiti nakon što se ponovno uspostavi rad informacijskog sustava, što može potrajati ukoliko je katastrofa (primjerice požar) prouzročila fizičku štetu na poslužiteljima, mrežnoj i ostaloj informatičkoj opremi.

Plan oporavka od katastrofe za podatkovni centar usmjeren je na zgradu u kojoj se nalazi podatkovni centar s poslužiteljima, mrežnom opremom i uređajima za pohranu podataka. Ovakav plan je skuplji za provedbu jer se pri njegovoj izradi trebaju uzeti u obzir fizička sigurnost, pričuvni izvori napajanja, pružatelji usluga mrežnih veza, planovi protupožarne zaštite. Međutim, vrijeme oporavka u slučaju katastrofe je manje jer će informatička oprema u pravilu biti sačuvana.

Plan oporavka od katastrofe moguće je i zakupiti od vanjskog pružatelja usluga. To se naziva **plan oporavka od katastrofe kao vanjska usluga (DRaaS)**. U tom slučaju cjelokupna IT infrastruktura organizacije (poslužitelji, uređaji za pohranu podataka, aplikacije, podatci) replicira se u virtualno okruženje (oblak). U slučaju katastrofe na glavnoj lokaciji informacijskog sustava organizacije, korisnici se mogu spojiti na kopiju IT infrastrukture u virtualnom okruženju korištenjem virtualnih privatnih mreža (engl. VPN) putem Interneta te nastaviti raditi u istom okruženju i na istim podatcima kao što bi radili na svom sustavu.

Neovisno o vrsti plana oporavka koji će se primijeniti u organizaciji, sukladno standardu 800-34 američkog National Institute of Standards and Technology on bi se trebao sastojati od tri faze [**6**]:

- aktivacija i obavješćivanje,
- oporavak
- obnova.

U prvoj fazi detektira se prekid rada sustava ili nastanak situacije koja je neizbježna, a koja će ga uzrokovati. Obavještava se ključno osoblje koje je zaduženo za reakciju i izvršenje plana, procjenjuje se važnost prekida na cjelokupno poslovanje, moguća šteta te duljina trajanja prekida.

U drugoj fazi započinju aktivnosti za oporavak funkcionalnosti sustava, popravak štete te nastavak rada na glavnoj ili pričuvnoj lokaciji. U toj fazi sudjeluje IT odjel/sektor odnosno cjelina koja se bavi administracijom informacijskog sustava, ali i cjelina koja se bavi informacijskom sigurnosti. Administratori osposobljavaju hardver, aplikacije, baze podataka

te vraćaju podatke iz pričuvnih kopija, a informacijska sigurnost brine se za sigurnost ponovno uspostavljenih mrežnih veza i sistemske infrastrukture [**12**].

Faza obnove podrazumijeva povratak informacijskog sustava u uobičajeno radno stanje. Obuhvaća validaciju podataka kojom se provjerava jesu li sačuvani svi podatci od posljednje izrađene pričuvne kopije podataka te jesu li uspostavljene sve funkcionalnosti. Po završetku te faze smatra se da informacijski sustav nastavlja normalno raditi.

Organizacija SHARE je zajedno s tvrtkom IBM tijekom 1980.-tih godina definirala 7 razina oporavka od katastrofe u IT području, od 0 do 6. Naknadno je dodana i razina 7 koja podrazumijeva potpuno automatizirani oporavak. Te razine su sljedeće [**15**]:

Razina 0 – bez pohrane podataka na pričuvnoj lokaciji

Podatci se ne pohranjuju na drugoj lokaciji, njihov povratak moguć je samo korištenjem sustava koji se nalaze na primarnoj lokaciji.

Razina 1 – Izrada pričuvne kopije podataka s hladnom lokacijom (engl. cold backup site)

Podatci se pohranjuju na diskove i fizičkim putem se šalju na pričuvnu lokaciju na kojoj ne postoje pričuvni sistemi nego samo osnovna infrastruktura poput namještaja, napajanja, mrežnih ormara i utičnica. U slučaju katastrofe na toj pričuvnoj lokaciji prvo je potrebno postaviti i instalirati odgovarajući hardver i softver. Tek nakon toga se s diskova koji su dostavljeni s primarne lokacije mogu prebaciti podatci od zadnje uspješno odrađene izrade pričuvne kopije podataka. Ovo rješenje je jeftino, ali nastavak rada obično je moguć tek nakon nekoliko dana.

Razina 2 – Izrada pričuvne kopije podataka s vrućom lokacijom (engl. hot backup site)

Podatci se pohranjuju na diskove i fizičkim putem se šalju na pričuvnu lokaciju na kojoj je instaliran i aktivan pričuvni sustav s odgovarajućim hardverom i softverom. Nakon toga se u sustav ubacuju podatci sačuvani s primarne lokacije. Ovo je skuplje rješenje, ali nastavak rada moguć je mnogo brže, obično do 24 sata.

Razina 3 – Elektronička pohrana

Podatci koji su kritični za poslovanje elektroničkim putem se šalju na vruću pričuvnu lokaciju. Ovo rješenje efikasnije je od prethodne dvije razine jer ne zahtijeva nikakav fizički

transfer pričuvnih kopija podataka. Nastavak rada u punom opsegu obično je moguć za desetak sati.

Razina 4 – Aktivna pričuvna lokacija

Svi podatci se periodički kopiraju s primarne na pričuvnu lokaciju i obrnuto elektroničkim putem. Ovakav pristup naziva se izradom kopija u „točki u vremenu“ (engl. point in time copies) i osigurava puno veću dostupnost (manji gubitak) podataka u slučaju katastrofe.

Razina 5 – Integritet transakcija

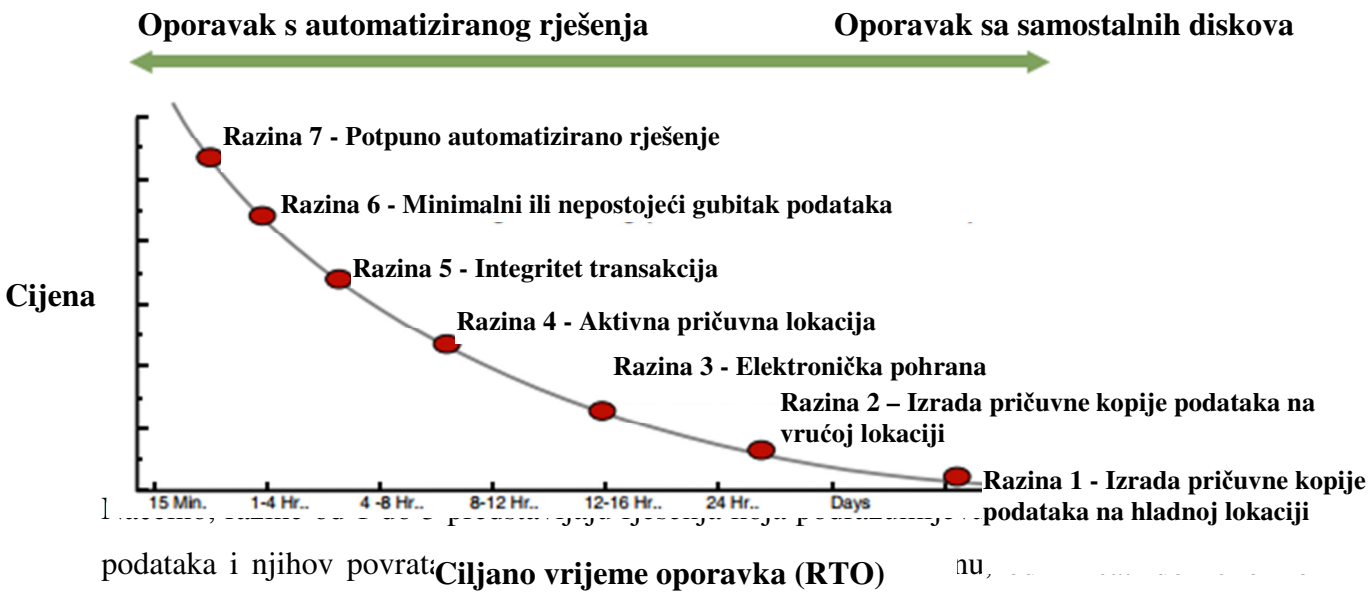
Aplikacijski podatci i podatci iz baza podataka se na transakcijskoj razini preslikavaju na diskove na pričuvnoj lokaciji. Ovisno o postavkama aplikacije, ovo rješenje omogućuje već gotovo potpuno očuvanje podataka u slučaju katastrofe.

Razina 6 – Minimalni ili nepostojeći gubitak podataka

Svi podatci (neovisno o kojoj aplikaciji se radi) se trenutno kopiraju s primarne na pričuvnu lokaciju elektroničkim putem, najčešće korištenjem tehnologija zrcaljenja diska (engl. disk-mirroring) ili replikacije diska.

Razina 7 – Potpuno automatizirano rješenje

Ovo je nadogradnja razine 6 pri kojoj u slučaju katastrofe informacijski sustav automatski nastavlja raditi na hardverskoj infrastrukturi, aplikacijama i podatcima koji se nalaze na pričuvnoj lokaciji bez ikakvog prekida ili gubitka podataka. Razine oporavka od katastrofe u IT području prikazane su na slici 9.

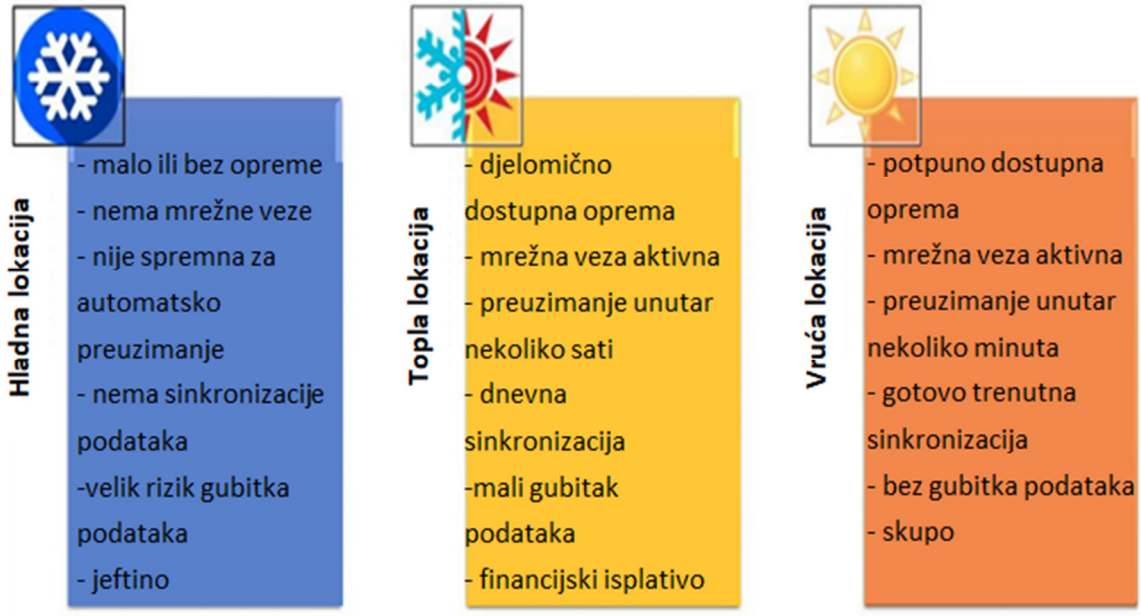


podataka i njihov povrat[illegible]nu,

Slika 9 – Razine oporavka od katastrofe u IT području [2]

dana. Razine 4 do 6 su rješenja koja podrazumijevaju brzi povratak podataka u slučaju katastrofe (nekoliko sati). Razina 7 sadrži rješenja koja osiguravaju stalnu dostupnost (gotovo) bez prekida u poslovanju.

Sve navedene razine oporavka od katastrofe, osim najlošije razine 0, podrazumijevaju da organizacija osim produkcijskog podatkovnog centra u kojem se nalazi ključna IT oprema, aplikacije i podatci treba imati najmanje još jednu fizičku ili virtualnu lokaciju na kojoj će se nalaziti pričuvna IT oprema i aplikacije ili barem kopija podataka. U slučaju incidenta odnosno neželjenog štetnog događaja na informacijskom sustavu koji prekida normalno poslovanje, informacijski sustav organizacije se osposobljava za rad na pričuvnoj lokaciji. Kako je prikazano na slici 10, te pričuvne lokacije mogu biti hladna, topla i vruća [**16**].



Slika 10 – Usporedba varijanti pričuvne lokacije podatkovnog centra [16]

Hladna pričuvna lokacija pruža samo osnovno fizičko okruženje odnosno prostor u kojem se u slučaju katastrofe na produkcijskoj (primarnoj) lokaciji mogu postaviti i instalirati poslužitelji i aplikacije, uspostaviti telekomunikacijske veze, a podatci vratiti iz medija s pričuvnom kopijom. Drugim riječima, na njoj nisu uspostavljeni pričuvni sistemi nego se tamo nalazi samo osnovna infrastruktura poput namještaja, napajanja, mrežnih ormara i utičnica. Korištenjem hladne pričuvne lokacije nije moguće ostvariti automatski prelazak rada sustava nego jedino ručni prelazak i to nakon odgovarajuće pripreme. Ovakvo rješenje ima velik RTO

i RPO te je pogodno jedino za sustave odnosno aplikacije koje nemaju zahtjev za visokom raspoloživosti. Jedina prednost ovog rješenja je niska cijena.

Topla pričuvna lokacija sadrži pripravne poslužitelje koji su spremni za pokretanje aplikacija u slučaju prekida na glavnoj lokaciji, ali su u "toplom" stanju, što znači da im treba određeno vrijeme kako bi postali aktivni. Aplikacije su instalirane, ali su baze podataka prazne. U slučaju katastrofe na primarnoj lokaciji, podatci se također trebaju vratiti iz medija sa pričuvnom kopijom. Prema tome, korištenjem ove lokacije također se ne može ostvariti automatski prelazak nego administratori moraju ručno izvršiti procedure za povratak aktualnih podataka. Ovakvo rješenje također podrazumijeva prekid u raspoloživosti (ima određeni RTO), ali mnogo kraći od onoga kada se koristi hladna lokacija.

Vruća pričuvna lokacija sadrži zrcalne (engl. mirroring) poslužitelje na kojima se nalaze sve aplikacije i podatci s produkcijske lokacije budući da se s nje gotovo trenutno sinkroniziraju odnosno repliciraju. Zrcalni poslužitelji su potpuno funkcionalni, na njima su instalirani operativni sustavi i aplikacije kakve postoje na poslužiteljima na produkcijskoj lokaciji. Troškovi za uspostavu vruće lokacije jako su visoki – na pričuvnoj lokaciji mora se nalaziti istovjetan hardver kao i na produkcijskoj, mrežne veze između te dvije lokacije stalno su aktivne, hardver je uključen što donosi troškove električne energije, na pričuvnoj lokaciji instaliran je sav softver kao i na glavnoj pa se moraju platiti dodatne licence. S druge strane, trajanje prekida u radu (RTO) i gubitak podataka (RPO) je minimalan ili ga uopće nema. Ovakvo rješenje nužno je za organizacije koje imaju potrebu za stalnom dostupnosti svojih usluga odnosno neprekidnosti poslovnog procesa kao što su banke i druge financijske institucije. Ono jedino omogućuje potpuno automatizirani prelazak rada sustava na pričuvnu lokaciju.

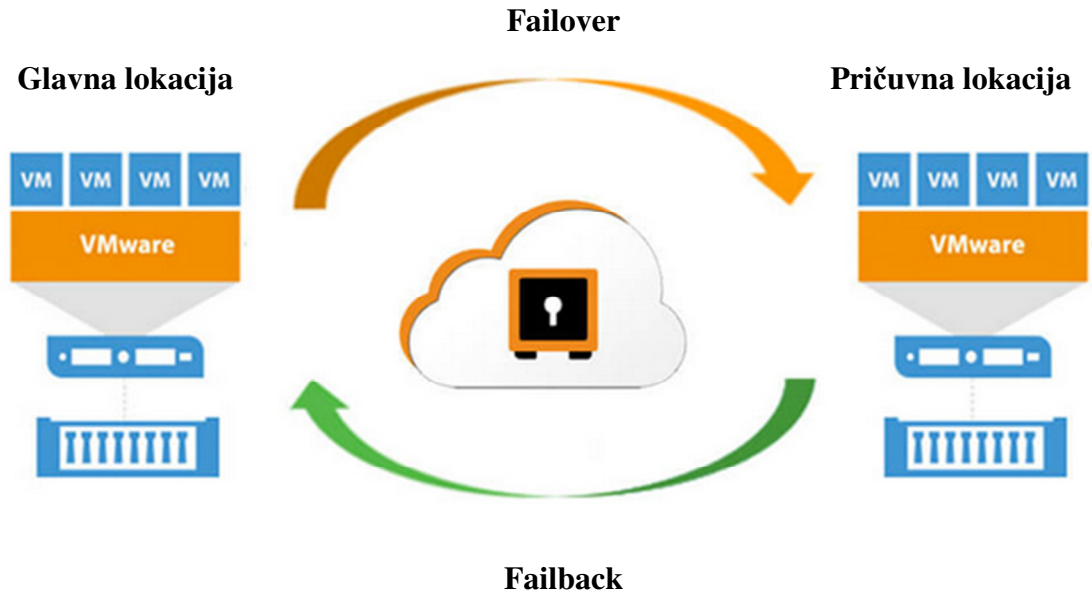
Procedure za prelazak rada s primarne na pričuvnu lokaciju u slučaju katastrofe te povratak na primarnu nakon oporavka nazivaju se (engl.) **failover**, **switchover** i **failback**.

Failover podrazumijeva automatski nastavak rada sustava na pričuvnom poslužitelju, hardverskoj ili mrežnoj komponenti u slučaju kvara ili nedostupnosti aplikacije, poslužitelja, hardverske ili mrežne komponente na primarnoj lokaciji [**17**]. Primjerice, kada jedan od dva Microsoft Exchange poslužitelja koji su podešeni u grupu (engl. cluster) postane nedostupan, baza podataka korisničkih sandučića (engl. mailbox database) koja se nalazi na drugom poslužitelju failover procedurom automatski će postati aktivna. Korisnici će nastaviti raditi na

toj bazi podataka. Moći će slati i primati elektroničku poštu te pregledavati svoje stare poruke te neće primijetiti da je jedan od poslužitelja postao nedostupan [**18**]. Pravi failover moguće je ostvariti jedino korištenjem vruće pričuvne lokacije na razini 7 oporavka od katastrofe prema definiciji organizacije SHARE u suradnji s tvrtkom IBM.

Varijanta failover procedure koja zahtjeva ljudsku intervenciju za prelazak rada aplikacije, poslužitelja, hardverske komponente ili mrežne komponente na drugu lokaciju naziva se **switchover**. Ta procedura u pravilu se koristi kao priprema za održavanje sustava u svrhu instalacije zakrpa te nadogradnje aplikacije ili operativnog sustava na novu verziju. Primjerice, na Exchange poslužiteljima koji su podešeni u cluster ova procedura može se koristiti za prelazak rada s jedne baze podataka na drugu (engl. database switchover) ili s jednog poslužitelja na drugi (engl. server switchover) [**18**]. Ova procedura također se može koristiti kao rješenje za prelazak na pričuvnu lokaciju u slučaju prekida rada na glavnoj lokaciji ukoliko je sustav prekompleksan za automatski prijelaz (failover) ili bi njegova implementacija bila preskupa [**19**]. U praksi se switchover koristi na razinama od 0 do 6 oporavka od katastrofe prema definiciji organizacije SHARE u suradnji s tvrtkom IBM.

Kada se informacijski sustav organizacije na glavnoj lokaciji (u produkcijskom podatkovnom centru) ponovno osposobi za rad, provodi se procedura povratka svih komponenti informacijskog sustava na glavnu lokaciju (engl. **failback**). Prilikom procedura povratka se s informacijskog sustava na pričuvnoj lokaciji na informacijski sustav na glavnoj lokaciji vraćaju promjene u podatcima i aplikacijama koje su nastale prilikom rada na sustavu na pričuvnoj lokaciji [**20**]. U idealnom slučaju, na razini 7 oporavka od katastrofe u IT području failback se izvršava automatski te nema gubitka podataka. U praksi gotovo uvijek dolazi do manjeg ili većeg gubitka, a rizik ovisi o primijenjenom rješenju za uspostavu pričuvne lokacije. Okvirna shema failover i failback procedura prikazana je na slici 11.

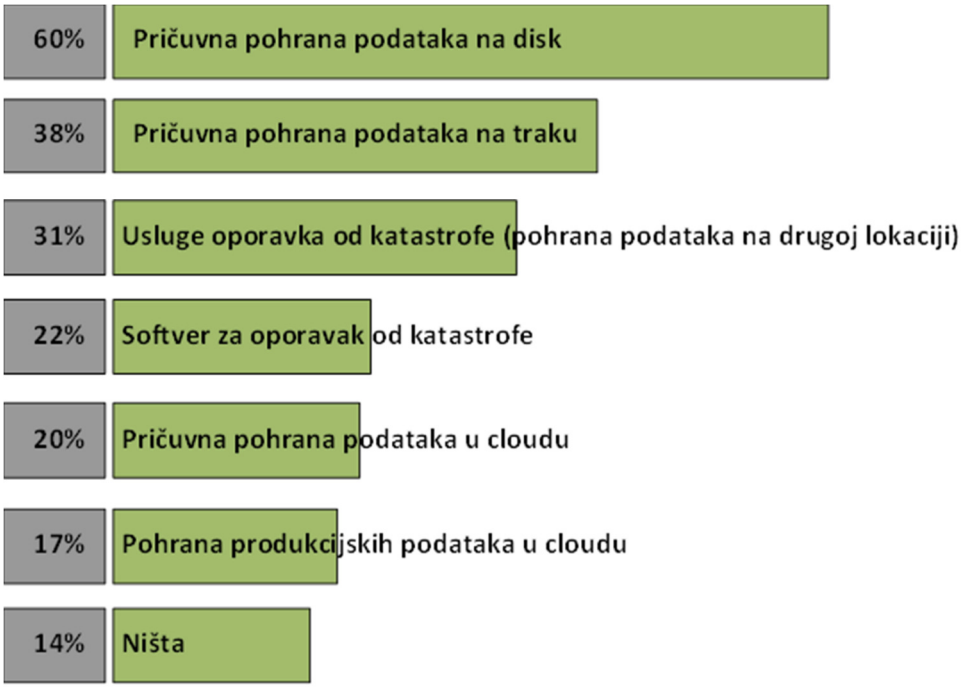


Slika 11 – Failover i failback [70]

U suvremenom IT okruženju, sve više organizacija prelazi na računarstvo u oblaku (engl. Cloud Computing). Oblak predstavlja skup računalnih resursa koji su dostupni korištenjem Interneta. Ti resursi mogu biti poslužitelji, uređaji za pohranu podataka, aplikacije i ostale usluge. Organizacija koja koristi računarstvo u oblaku ne mora kupovati vlastite nego može iznajmiti tuđe računalne resurse koji su dostupni u oblaku. Jedna od mogućnosti računarstva u oblaku je i oporavak od katastrofe kao vanjska usluga (DRaaS). Organizacija koja koristi tu uslugu replicira aplikacije i podatke iz svog podatkovnog centra u oblak. U slučaju kada zbog izvanrednog događaja on postane nedostupan, aplikacije s aktualnim podatcima dostupne su u oblaku, a za pristup na njih dovoljna je Internetska veza i Web preglednik. Prema tome, prilikom failovera gotovo da uopće nema prekida poslovnog procesa. U praksi oblak za organizaciju predstavlja vruću pričuvnu lokaciju koja je virtualna – organizacija nema stvarni pričuvni prostor, hardver, aplikacije i mrežne veze nego se sva ta infrastruktura zakupljuje od velikih tvrtki koje pružaju usluge oblaka. Nakon što organizacija sanira štetu i osposobi svoj produkcijski podatkovni centar, failback se provodi replikacijom aplikacija i promjena u podatcima iz oblaka natrag na njega nakon čega organizacija nastavlja koristiti vlastite računalne resurse. Korištenjem oblaka najjednostavnije se i financijski najpovoljnije može postići razina 7 za oporavak od katastrofe u IT području.

2.5.3. Komercijalni alati za oporavak od katastrofe

Većina organizacija (poslovnih subjekata, državnih tijela, industrija, uslužnih djelatnosti) u svom poslovanju koristi barem jedno od nekoliko mogućih alata za oporavak od katastrofe u IT području. Najjednostavnija tehnika za oporavak je izrada pričuvne pohrane podataka, ali sama po sebi nije dovoljna. Iz tog razloga sve više se koriste vanjske usluge oporavka od katastrofe, specijalizirani softver te pohrana podataka u oblaku [**21**]. Prikaz alata i tehnika za oporavak od katastrofe u IT području prikazan je na slici 12.

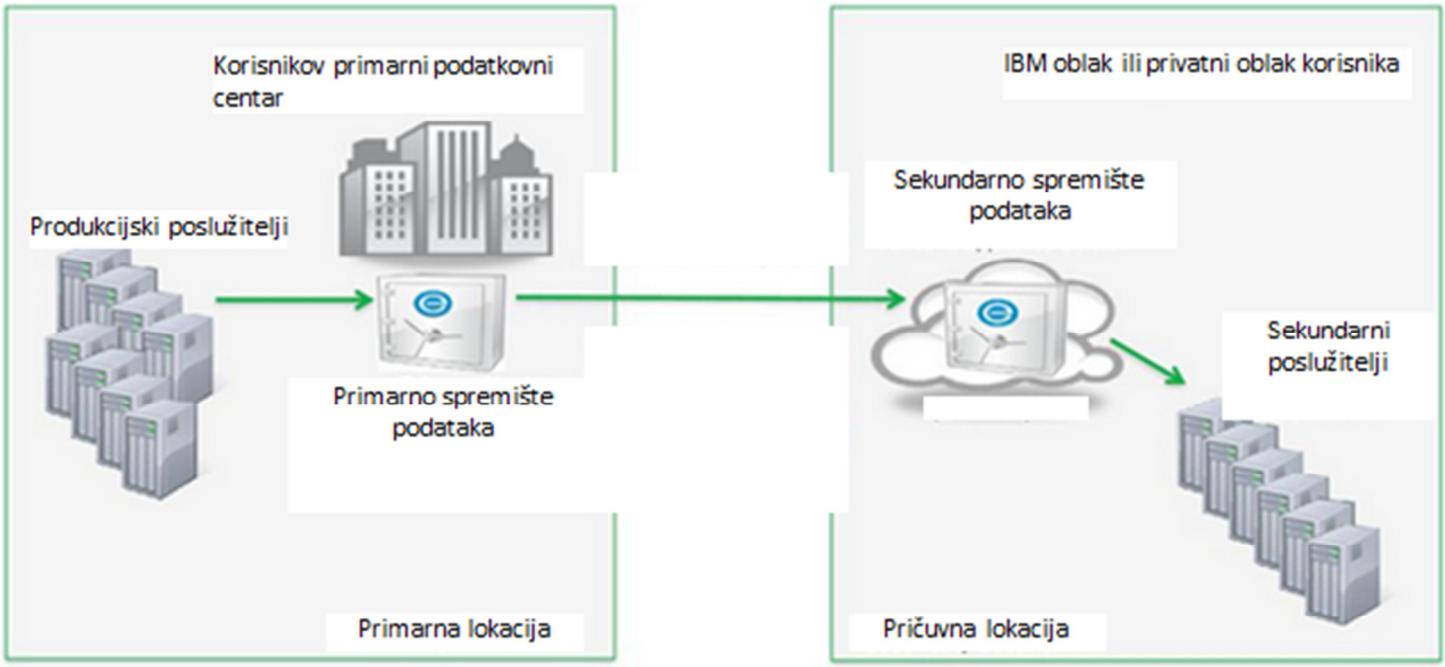


Slika 12 – Alati i tehnologije za oporavak od katastrofe u IT području [21]

Slijedom navedenog vidljivo je kako su u suvremenim poslovnim okruženjima usluge oporavka od katastrofe u IT području (DRaaS) važan segment IT tržišta te su u stalnom rastu. Prema određenim tržišnim predviđanjima, globalno tržište DRaaS usluga porast će s 5,1 milijarde USD u 2020. na 14,6 milijardi USD u 2025. godini. Tim tržištem dominiraju tvrtke Microsoft, IBM, VMware, Acronis i Recovery Point [**22**]. Neka od poznatijih DRaaS rješenja su sljedeća:

IBM Backup as a Service (BaaS) [**23**] prikazan na slici 13 je rješenje koje se temelji na pohrani podataka i aplikacija u javnom IBM oblaku ili u privatnom oblaku korisnika u njegovom fizičkom podatkovnom centru na pričuvnoj lokaciji. U slučaju katastrofe odnosno incidenta u kojem informacijski sustav korisnika postaje nedostupan korisnici nastavljaju

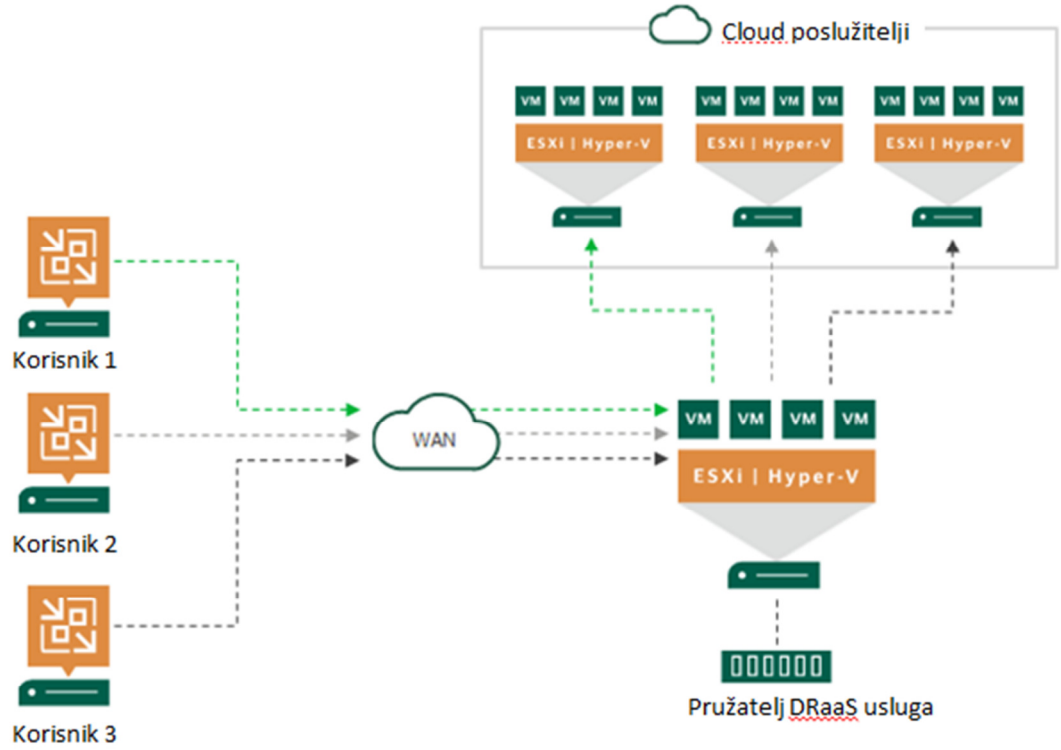
raditi u oblaku dok se u pozadini provodi oporavak sustava. Rješenje nudi i zaštitu od kibernetičkih napada usmjerenih na korupciju podataka i ucjenjivački softver.



Slika 13 - Usluga IBM BaaS [23]

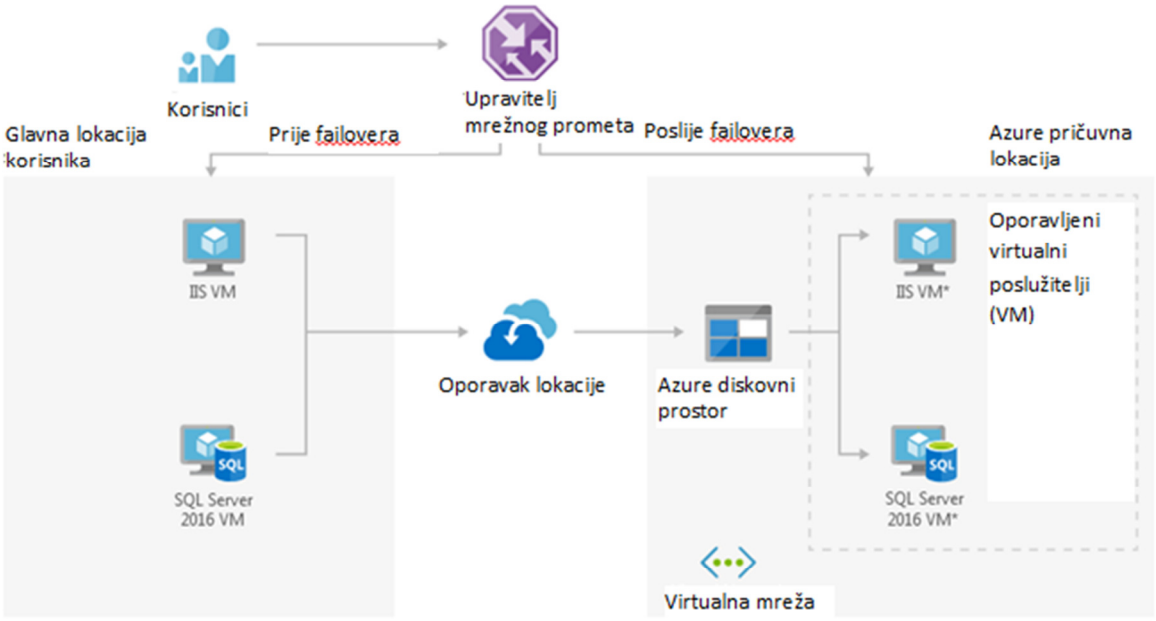
Veeam Cloud Connect Replication [**24**] prikazan na slici 14 je nadogradnja na **Veeam Backup** koji je jedan od najpoznatijih alata za izradu pričuvne kopije (backup) virtualnih poslužitelja instaliranih na VMware ESXi ili Microsoft Hyper-V hipervizoru. Hipervizor je virtualizacijska tehnologija koja se sastoji od fizičkog poslužitelja i softvera. Služi za upravljanje virtualnim poslužiteljima koji su kreirani i pokrenuti na njemu [**25**]. ESXi od tvrtke VMware i Hyper-V od tvrtke Microsoft su najkorišteniji hipervizori na globalnoj razini. Veeam Cloud Connect Replication rješenjem virtualni poslužitelji s lokacije korisnika repliciraju se u oblak kod nekog pružatelja DRaaS usluga. U slučaju katastrofe na lokaciji korisnika, prelazi se na rad na replikama virtualnih poslužitelja u oblaku. Ukoliko se sruše kritični poslužitelji korisnika izvršit će se automatski potpuni (engl. full-site) failover na poslužitelje u oblaku. Ukoliko samo jedan ili nekoliko manje važnih poslužitelja postane nedostupno izvršit će se automatski djelomični (engl. partial-site) failover na poslužitelje u oblaku. Taj prostor tada predstavlja virtualnu vruću pričuvnu lokaciju korisnikovog

informacijskog sustava. Kada korisnik otkloni problem na svojoj lokaciji, može pokrenuti proceduru povratka virtualnih poslužitelja iz oblaka na svoju lokaciju (failback).



Slika 14 - Usluga Veeam Cloud Connect Replication [24]

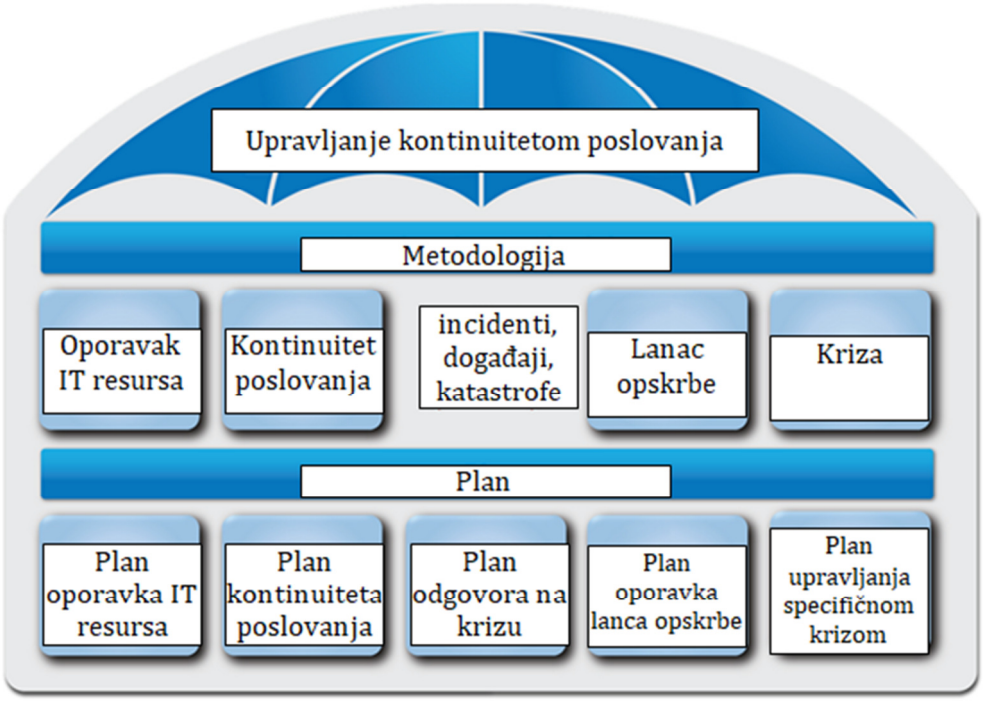
Microsoft Azure Site Recovery [**26**] prikazan na slici 15 u kombinaciji s **Azure Backup** također nudi oblak, ali i lokalno rješenje za izradu pričuvnih kopija podataka. Korištenjem tog rješenja korisnik može vlastite fizičke i virtualne poslužitelje replicirati u Azure oblaka na jednoj ili više regija te na drugu fizičku lokaciju. Slično kao i rješenja od IBM-a i VEEAM-a u slučaju katastrofe nude se mogućnosti za automatski failover te naknadni failback uz neprekidni rad korisnika u oblaku.



Slika 15 - Usluga Microsoft Azure Site Recovery [26]

2.6. Upravljanje kontinuitetom poslovanja

Upravljanje kontinuitetom poslovanja (engl. Business Continuity Management, BCM) obuhvaća razvoj strategija, planova i aktivnosti koje osiguravaju alternativne načine djelovanja za one djelatnosti i procese čiji bi prekid mogao izazvati značajne štete i gubitke za organizaciju. BCM kao proces prepoznaje utjecaje prijetnji na poslovanje organizacije i služi za izradu planova odgovora. On daje odgovor na pitanje „Što će se dogoditi ako kontrole zakažu?“ i usko je vezan uz proces upravljanja rizicima u organizaciji. Predstavlja aktivni preventivni pristup kojim se nastoji osigurati da se kritične poslovne funkcije nastave odvijati nakon prekida poslovanja bilo koje vrste. Drugim riječima, ključni cilj tog procesa je povećati otpornost organizacije na poremećaje poslovanja i umanjiti utjecaj takvih poremećaja [**27**].

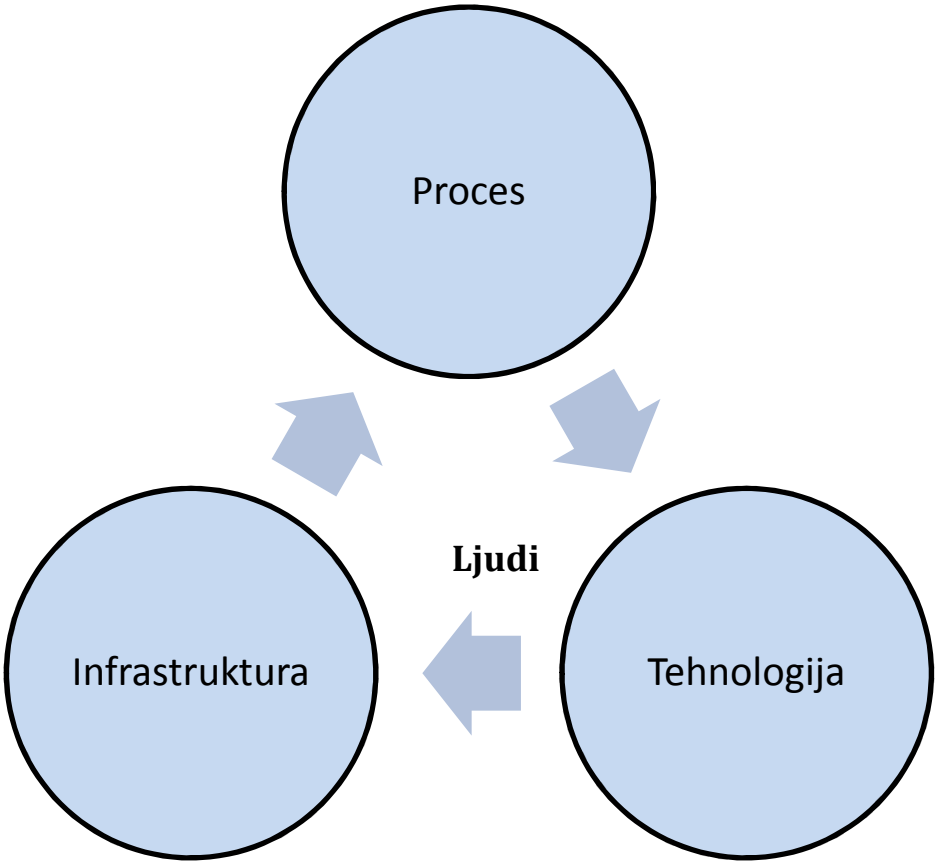


Slika 16 - „Kišobran“ upravljanja kontinuitetom poslovanja [28]

Komponente upravljanja kontinuitetom poslovanja prikazane su na slici 16. Potencijalne prijetnje mogu ugroziti neprekidnost (kontinuitet) poslovanja, ali također i neprekidnost lanca opskrbe te raspoloživost IT resursa. Primjenom određene metodologije razvijaju se planovi kojima se minimiziraju negativni učinci prijetnji poslovanju te osigurava neprekidnosti poslovnih procesa [**28**].

Poslovanje organizacije može se promatrati na različite načine, ali u svrhu planiranja kontinuiteta poslovanja važna su tri elementa: ljudi, procesi i tehnologija koja uključuje i

infrastrukturu. Na slici 17 koja prikazuje interakciju elemenata poslovanja infrastruktura je prikazana zasebno zbog preglednosti. Tehnologijom se služe ljudi kroz određene poslovne procese. Učinkovitost tehnologije ovisi o stupnju obučenosti ljudi koji ju koriste te o razrađenosti procesa u kojima se koristi. A što je proces bolje definiran, njegovi rezultati su pouzdaniji [**8**].



Slika 17 – Interakcija elemenata poslovanja [8]

Ljudi su najvažnija sastavnica planiranja kontinuiteta poslovanja. Oni izrađuju planove te ih provode u slučaju katastrofalnih događaja odnosno bilo kakvih neočekivanih štetnih događaja koji mogu prouzročiti prekid poslovanja. Što se tiče takvih događaja u IT segmentu, za 40% pa čak do 80% slučajeva [**8**] gubitka podataka odgovorni su upravo ljudi. Iako u svakoj IT infrastrukturi postoje procedure za izradu pričuvnih kopija te povratak izgubljenih podataka, ljudi i dalje čine pogreške koje uzrokuju gubitak podataka.

Prilikom izrade plana kontinuiteta poslovanja, važno je da u njemu sudjeluju djelatnici iz različitih dijelova organizacije. Primjerice, informatičari mogu pripremiti kvalitetan plan za oporavak u slučaju kvara glavnih poslužitelja, ali sami ne mogu izraditi plan kontinuiteta poslovanja odjela za financije budući da ne poznaju poslovne procese izvan vlastitog djelokruga. Jedino uz sudjelovanje djelatnika iz različitih cjelina može se izraditi sveobuhvatan plan koji pokriva cjelokupno poslovanje organizacije. Prema tome, u njemu moraju biti imenovani ključni ljudi za njegovu provedbu iz svih kritičnih područja poslovanja.

Unutar organizacije redovite poslovne aktivnosti provode se kroz definirane poslovne procese. Poslovni događaji koji nisu pokriveni procesima obično se rješavaju pojedinačno, kao iznimke, dok ne postanu dovoljno učestali da se za njih definira novi proces. Ako je poslovanje pogođeno katastrofalnim događajem velikih razmjera poput požara, poplave ili potresa, svi poslovni procesi u pravilu će biti zaustavljeni. Vrijeme koje je potrebno da se postojeći poslovni procesi preoblikuju odnosno prilagode kako bi se poslovanje organizacije moglo nastaviti zavisno je od aktivnosti koje su definirane za provedbu plana kontinuiteta poslovanja. Prema tome, taj plan treba predvidjeti što više mogućih različitih tipova neočekivanih štetnih događaja i katastrofa te imati razrađene aktivnosti kojima će se nastaviti poslovanje ako se isti dogode. Za izradu kvalitetnog plana nužno je analizirati i dokumentirati postojeće poslovne procese te ih razvrstati prema važnosti. Neki od njih su kritični za poslovanje organizacije, a drugi mogu biti zaustavljeni na kraći ili dulji rok. U planu je također potrebno predvidjeti scenarije za neočekivane štetne događaje i katastrofe u različitim vremenskim segmentima poslovanja. Tako, primjerice, za poslovanje organizacije nije svejedno je li se neočekivani štetni događaj poput nestanka struje u podatkovnom centru (engl. data centar) dogodio prije, za vrijeme ili nakon isplate plaće.

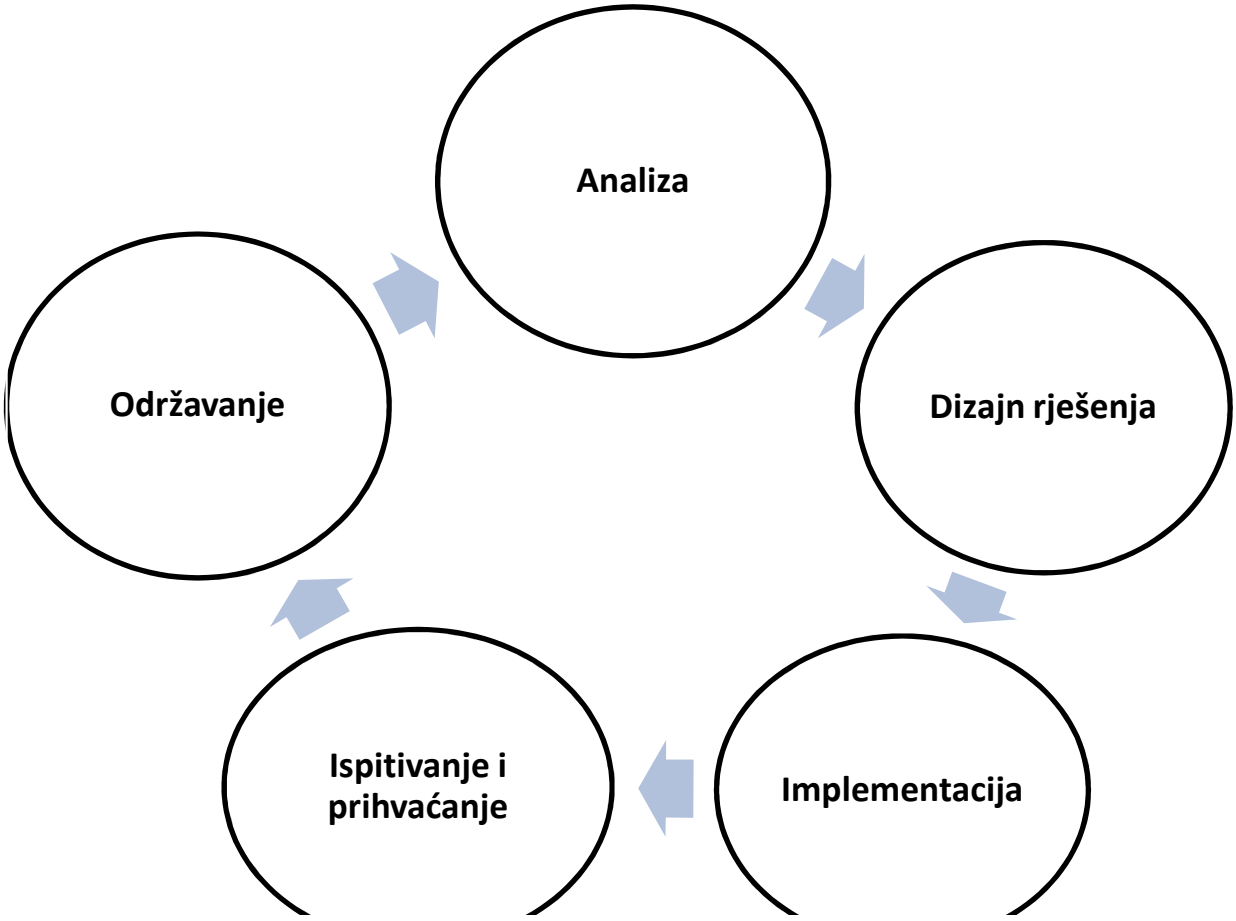
Tehnologija i infrastruktura međusobno su isprepletene i koriste se u svim segmentima poslovanja. Najizravnije su podložne štetnim događajima poput nestanka struje, požara ili poplave. Određena tehnologija izravno je uključena u poslovne procese (primjerice korisnička računala s pristupom na računovodstvenu aplikaciju), a druga je u funkciji osiguravanja kontinuiteta poslovanja (primjerice pričuvni podatkovni centar na drugoj lokaciji). Plan kontinuiteta poslovanja mora voditi računa o obje te vrste tehnologije na uporabi u organizaciji, osobito zato što je sva tehnologija koja se koristi u poslovanju organizacije uvezana i međuzavisna.

2.6.1. Metodologija planiranja kontinuiteta poslovanja

Plan kontinuiteta poslovanja mora biti izrađen tako da bude realističan i da se tijekom krize može koristiti na jednostavan način. Osnovni dio izrade plana kontinuiteta poslovanja je određivanje najdužeg ciljanog vremena oporavka (RTO) odnosno vrijeme unutar kojeg se poslovni procesi moraju ponovno uspostaviti. RTO se određuje u fazi analize odnosno u prvoj fazi izrade plana kontinuiteta poslovanja. Potrebno je napomenuti da je RTO cilj, a ne točno određena vrijednost. Stoga će u praksi vrlo često biti odabrana strategija koja neće uspjeti dostići RTO, no on svejedno ostaje cilj sljedeće revizije strategije. Stvarna vrijednost u ovom kontekstu naziva se RTA (engl. recovery time actual, RTA), dok se razlika do RTO naziva "gap". Do stvarne RTA vrijednosti se dolazi simulacijama ili vježbama, odnosno empirijski, u slučaju nastupa stvarnog prekida poslovanja.

Načelne faze izrade plana kontinuiteta poslovanja prikazane na slici 18 su sljedeće [**29**]:

1. analiza,
2. dizajn rješenja,
3. implementacija,
4. ispitivanje i prihvaćanje od strane organizacije,
5. održavanje prihvaćenog plana.



Slika 18 – Faze izrade plana kontinuiteta poslovanja [8]

U **fazi analize** izrađuje se analiza utjecaja na poslovanje (BIA) te procjena rizika. Svrha provedbe analiza utjecaja prekida poslovnih procesa na poslovanje jedne organizacije jest utvrditi koji su poslovni procesi ključni za preživljavanje organizacije u slučaju incidenta većih razmjera, kao i određivanje prioriteta njihove obnove. Tijekom provedbe ove analize prikupljaju se podatci koji su ključni za odabir strategije kontinuiteta poslovanja, implementaciju rješenja te izradu planova i procedura kontinuiteta poslovanja. Spomenuti podatci, između ostaloga, uključuju:

- identifikaciju ključnih poslovnih procesa i scenarija koji ih mogu ugroziti,
- opipljive i neopipljive troškove uzrokovane prekidom procesa,
- RTO,
- RPO,
- minimalnu razinu usluge koja je prihvatljiva za postizanje poslovnih ciljeva tijekom prekida.

Prekid odvijanja ključnih procesa za izravnu posljedicu ima pojavu troškova u odnosu na uobičajeno, neometano poslovanje jedne organizacije. Pri tome razlikujemo dvije osnovne vrste troškova – opipljive i neopipljive. U opipljive troškove ubrajaju se oni troškovi koje je moguće kvantitativno iskazati. Najčešće je riječ o financijskim troškovima (smanjenje ili kašnjenje prihoda, povećani operativni troškovi i sl.), budući da je njih u većini slučajeva moguće procijeniti analizom poslovanja organizacije. Od ostalih vrsta opipljivih troškova valja izdvojiti smanjenje usluga u ponudi, gubitak tržišnog udjela, smanjenje broja korisnika i slično. Neopipljivi troškovi su oni koje nije moguće kvantitativno prikazati, ali imaju značajan utjecaj na buduće poslovanje organizacije. To su, primjerice, gubitak ugleda, gubitak povjerenja korisnika, smanjenje konkurentnosti i slično. Za sve identificirane troškove potrebno je odrediti razinu utjecaja na poslovanje. Svaka organizacija definira koje od navedenih parametara će procjenjivati pri provedbi analize utjecaja prekida poslovnih procesa na poslovanje, kao i koliko razina utjecaja će pri tome koristiti. Za razine utjecaja može se koristiti kvalitativni pristup, pri čemu se opisno definira što znači svaka razina (niska, srednja, visoka), kao i kvantitativni pristup. Ovaj pristup podrazumijeva financijski izračun posljedica prekida ključnih poslovnih procesa. U praksi je moguće koristiti i kombinaciju ova dva pristupa: kvantitativni za procjenu opipljivih troškova, a kvalitativni za procjenu neopipljivih troškova. Kao rezultat ove faze dobiva se jasna podjela između kritičnih i nekritičnih funkcija u organizaciji. Poslovna funkcija se smatra kritičnom, ako utjecaj realizacije nekog

neočekivanog štetnog događaja ima neprihvatljive posljedice po nju i po interese organizacije ili ukoliko je takvom definira zakonska legislativa. Analizom utjecaja na poslovanje procjenjuje se koliko si vremena organizacija može dopustiti da joj pojedini ključni poslovni procesi (primjerice naplata usluge, sučelje za pristup na online trgovinu) ne funkcioniraju. Analizom prijetnji identificiraju se prijetnje poslovanju organizacije i daje se procjena vjerojatnosti njihove pojave. Tu se obrađuju događaji poput zemljotresa, požara, poplave, dugotrajnog nestanka električne energije, napada na informatički sustav organizacije i slično. Pri izradi scenarija utjecaja dokumentiraju se utjecaji prijetnji na poslovanje organizacije odnosno sve bitno vezano uz kontinuitet poslovanja u slučaju incidenta – osobe ključne za povratak poslovanja, prihvatljivo vrijeme prekida poslovanja, aplikacije i podatci koji moraju biti dostupni za funkcioniranje kritičnih poslovnih funkcija, rješenja za privremeno otklanjanje nastalih problema i slično.

U **fazi dizajna** definira se troškovno najpovoljnije rješenje oporavka od katastrofe. Ono u sebi pomiruje dva osnovne zahtjeva iz prethodne faze, a to su analiza prijetnji i scenariji utjecaja. U ovoj fazi razrađuju se konkretne mjere kojima se organizira oporavak poslovanja (engl. business recovery organization). Rezultat ove faze je stvaranje procedura za eskalaciju i aktivaciju plana oporavka s fokusom na kritične poslovne funkcije organizacije.

U **fazi implementacije** se navedene procedure provode u djelo (u stvarnom slučaju neočekivanog štetnog događaja), odnosno provodi se njihovo testiranje u kontroliranim uvjetima što uključuje i trening djelatnika organizacije uključenih u njegovu provedbu.

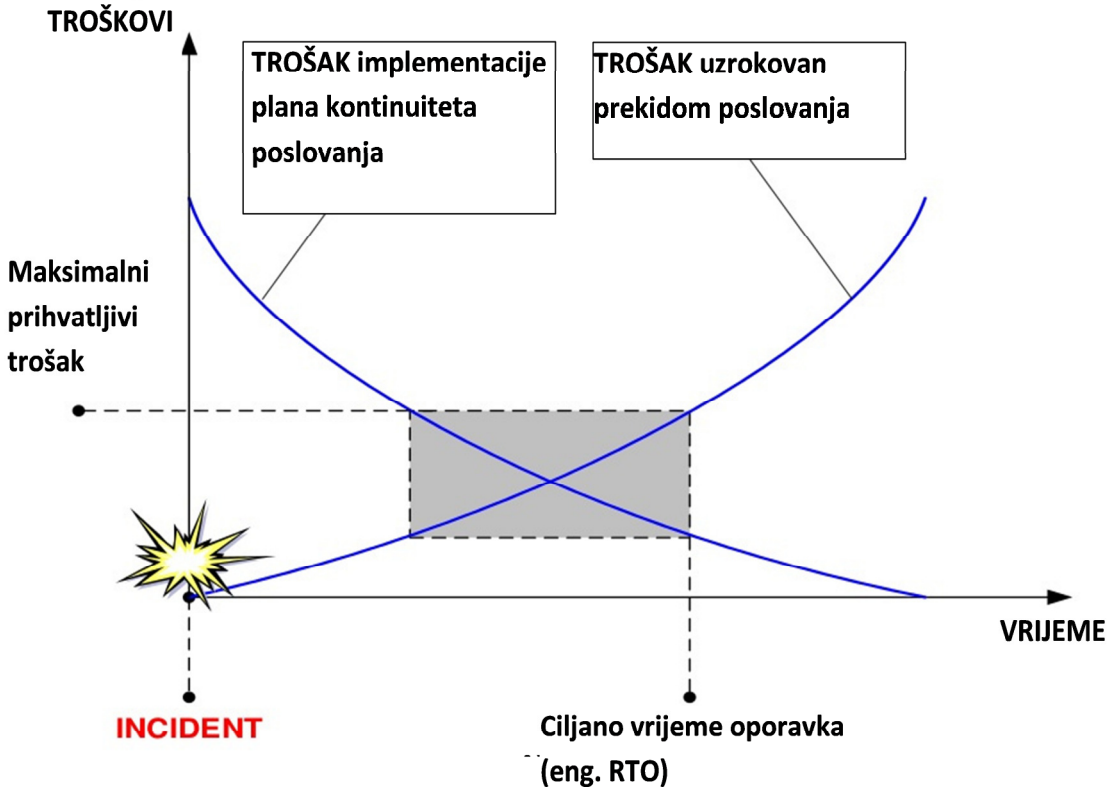
U **fazi ispitivanja** provodi se testiranje cjelokupnog rješenja za kontinuitet poslovanja, ali i provjera njegove usklađenosti sa zakonskom regulativom, te ciljevima, politikama i etičkim stavovima organizacije. Tako, primjerice, mjera oporavka od katastrofe koja podrazumijeva prebacivanje poslovanja na izdvojenu lokaciju udaljenu 100 km od glavne lokacije može biti cjenovno i organizacijski prihvatljiva, ali može predstavljati veliki problem za zaposlenike organizacije. Tek kad rješenje bude prihvatljivo po svim relevantnim kriterijima, a ne samo tehničkim ili financijskim, organizacija ga može prihvatiti i ugraditi u svoju poslovnu politiku.

U završnoj **fazi održavanja** prihvaćenog plana organizacija vodi brigu da s planom kontinuiteta budu upoznati svi zaposlenici, da osobe koje su kritične za njegovu provedbu

prolaze periodičke treninge za njegovu provedbu te da se provode periodička testiranja procedura za kontinuitet poslovanja i oporavak od katastrofe koje su dokumentirane u planu.

2.6.2. Troškovi implementacije plana kontinuiteta poslovanja

Pri izradi plana kontinuiteta poslovanja nužno je poznavati troškove prekida poslovanja, a koji se procjenjuju u prvoj, fazi analize. Visina ulaganja u plan i procedure za održavanje kontinuiteta poslovanja izravno ovisi o njima. Primjerice, jedna studija iz siječnja 2016. godine provedena u SAD na organizacijama koje su imale ukupno 63 vlastita podatkovna centra, a koje su imale prekide u radu u prethodnih 12 mjeseci pokazala je kako su prosječni troškovi po minuti nedostupnosti bili 8.851 USD. Prosječni ukupni troškovi nedostupnosti podatkovnih centara u cijelom promatranom razdoblju bili su 740.357 USD. U istoj takvoj studiji provedenoj 2010. godine prosječni troškovi prekida poslovanja odnosno nedostupnosti podatkovnih centara bili su 505.502 USD odnosno za oko 32% manji [**30**]. Iako se obje navedene studije odnose na organizacije odnosno poduzeća iz IT područja, s obzirom na sveopću informatizaciju poslovanja odnosno potrebu da ono bude dostupno 24/7 kako u privatnom, tako i u javnom sektoru, može se zaključiti kako prekidi poslovanja u svim djelatnostima nose velike troškove.



Slika 19 – Odnos troška uzrokovanog prekidom poslovanja i troška implementacije plana kontinuiteta poslovanja [13]

Troškovi planiranja kontinuiteta poslovanja vezani su uz tri primarna aspekta koje se tim planom žele ostvariti, a to su visoka dostupnost usluga, neprekidnost poslovanja i oporavak od katastrofa. To zahtjeva ulaganja u infrastrukturu, tehnologiju (informatičku i drugu), procedure, vanjske usluge i ljudski rad, a to sve za organizaciju predstavlja trošak. Prema tome, prilikom izrade plana kontinuiteta poslovanja treba se pronaći sredina između troškova uzrokovanog prekidom poslovanja i troškova implementacije plana kontinuiteta poslovanja [**13**]. Odnos tih dvaju tipova troškova prikazan je na slici 19.

2.6.3. Upravljanje kontinuitetom poslovanja u IT području

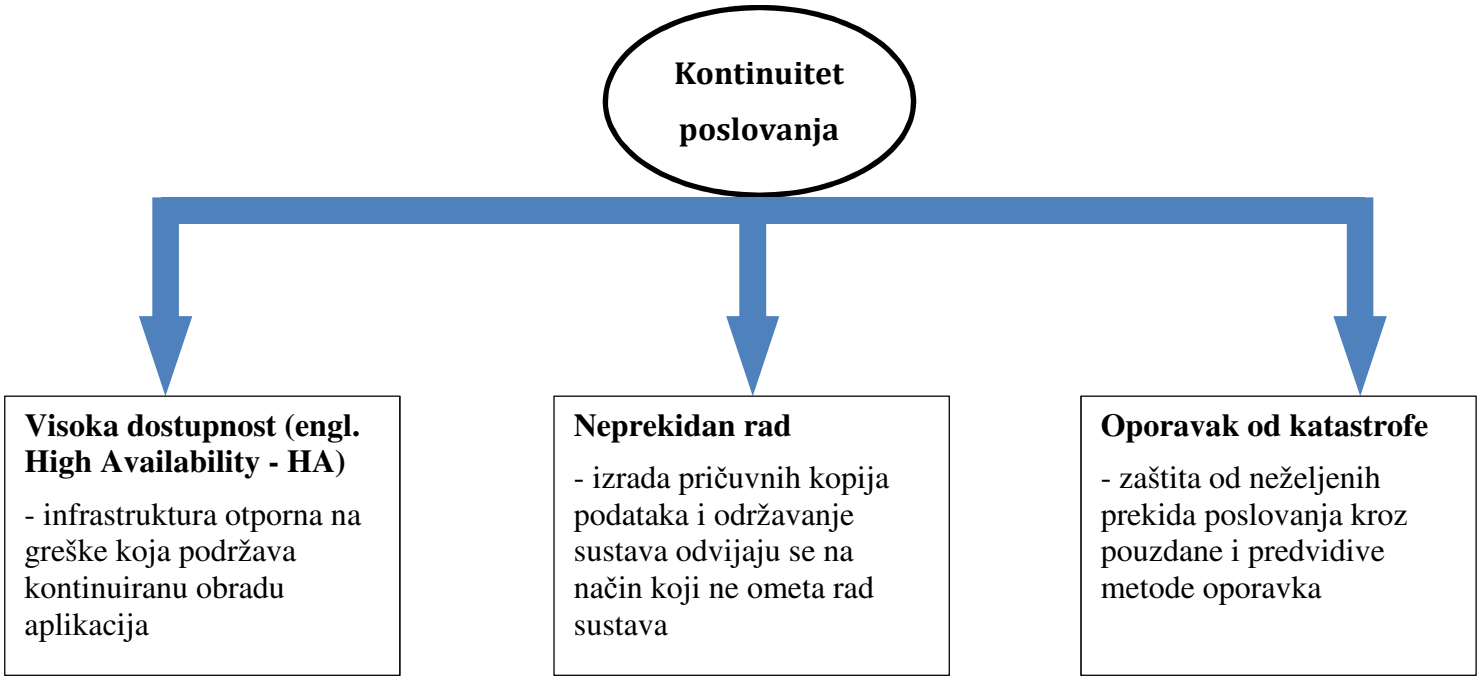
Plan upravljanja kontinuitetom poslovanja u IT području mora osigurati da kritične IT usluge budu dostupne korisnicima i prilikom nastanka katastrofe čime će se poslovanje nastaviti, makar u smanjenom obliku. On treba sadržavati [**31**]:

- procedure kojima će se omogućiti neprekidnost u isporuci kritičnih IT usluga,

- popis resursa neophodnih za kontinuitet poslovanja iz IT perspektive; takav popis sadrži kritičnu opremu, osoblje, lokacije te vanjske usluge vezane uz IT.

Organizacija koja ima ovakav plan imat će manju financijsku štetu kad se dogodi katastrofa koja narušava poslovanje, ali će imati i pozitivniju sliku (engl. image) kod svojih klijenata i dioničara koji će zbog njegovog postojanja znati da je organizacija proaktivna u zaštiti svoga poslovanja, a i njihovih interesa.

Kako je prikazano na slici 20, kontinuitet poslovanja u IT području sastoji se od tri međusobno povezane, ali ipak različite sastavnice. To su **visoka dostupnost**, **neprekidan rad** i **oporavak od katastrofe** [**2**].



Slika 20 – Sastavnice kontinuiteta poslovanja u IT području [2]

Visoka dostupnost podrazumijeva dostupnost aplikacija neovisno o lokalnim problemima u radu, bilo da su uzrokovani poslovnim procesima, tehničkim kvarovima ili greškama na softveru i hardveru. S gledišta informacijske tehnologije ona se osigurava redundancijom softvera i hardvera čime se uklanja mogućnost jedne točke kvara (engl. single point of failure).

Neprekidan rad znači da je informacijski sustav uvijek dostupan u situacijama kada sve radi kako treba. Sve aktivnosti održavanja sustava poput izrade pričuvnih kopija podataka,

instalacije sigurnosnih zakrpa te novih verzija operativnih sustava i softvera provode se na način koji ne prekida dostupnost aplikacija.

Oporavak od katastrofe podrazumijeva mogućnost oporavka informacijskog sustava na drugom hardveru te, često, na drugoj lokaciji ukoliko je katastrofa uništila ili onesposobila primarnu lokaciju gdje se informacijski sustav nalazi.

Uspostava kontinuiteta poslovanja u IT području provodi se kroz određeni set aktivnosti koje treba slijedno izvršiti [**2**]:

1. nabava pouzdane hardverske infrastrukture – mrežna oprema, poslužitelji, uređaji za pohranu podataka. Infrastrukturu treba podesiti tako da nema jedne točke kvara,
2. instalacija operativnih sustava, firmwarea, te aplikacijskih alata za upravljanje sustavom, izradu pričuvnih kopija podataka i ostale temeljne funkcije,
3. integracija poslužitelja u svrhu podešavanja automatskih procedura provjere sistemskih zapisa (engl. event log) te izrade pričuvnih kopija stanja poslužitelja (engl. snapshot),
4. integracija aplikacija za upravljanje diskovnim prostorima, bazama podataka, procedurama za visoku dostupnost te oporavak od katastrofe.

3. Oporavak od katastrofe u izoliranom informacijskom sustavu

Organizacije koje upravljaju izoliranim informacijskim sustavima susreću se sa specifičnim izazovima u smislu kontinuiteta poslovanja odnosno oporavka od katastrofe u IT području. Za razliku od otvorenog, izolirani ili zatvoreni informacijski sustav nema nikakvu interakciju sa svojim okruženjem odnosno s drugim informacijskim sustavima. Njega koriste organizacije koje zbog sigurnosnih ili zakonskih aspekata svoga poslovanja moraju izolirati svoj informacijski sustav od drugih, nesigurnih informacijskih sustava poput Interneta. Takav sustav može sadržavati klasificirane podatke ili upravlja osjetljivim poslovnim procesom poput kontrole leta ili upravljanja postrojenjem nuklearne elektrane. Kao i svaki drugi informacijski sustav i izolirani sustav sastoji se od poslužitelja, mrežne opreme, uređaja za pohranu podataka te instaliranih aplikacija. Sva ta oprema nalazi se u prostoru koji koristi organizacija. Njegova mrežna oprema služi za uvezivanje računala i poslužitelja u lokalnoj računalnoj mreži na glavnoj lokaciji (engl. Local Area Network, LAN) te za uvezivanje udaljenih lokacija s glavnom lokacijom (engl. Wide Area Network, WAN – mreža širokog područja), ali **nema vezu prema Internetu** ili drugim informacijskim sustavima. Zbog toga u izoliranom informacijskom sustavu **nije moguće raditi sigurnosnu pohranu podataka u oblaku (izvan sustava) ni zakupiti DRaaS uslugu od vanjskog pružatelja usluga**.

Osjetljivost izoliranog sustava proizlazi iz toga što je fizički vezan na određenu lokaciju. Osnovni elementi koji su podložni katastrofama su fizički objekt, okolina (napajanje, klimatizacija), požarna zaštita, kontrole pristupa, IT infrastruktura [**32**]. U praksi su najčešće katastrofe na IT infrastrukturi uzrokovanim ljudskim djelovanjem. Takve katastrofe mogu imati unutarnje uzroke kao što je gubitak podataka uzrokovan nepažnjom zaposlenika organizacije ili vanjske – prestanak rada poslužitelja uzrokovan zlonamjernim softverom (engl. malware).

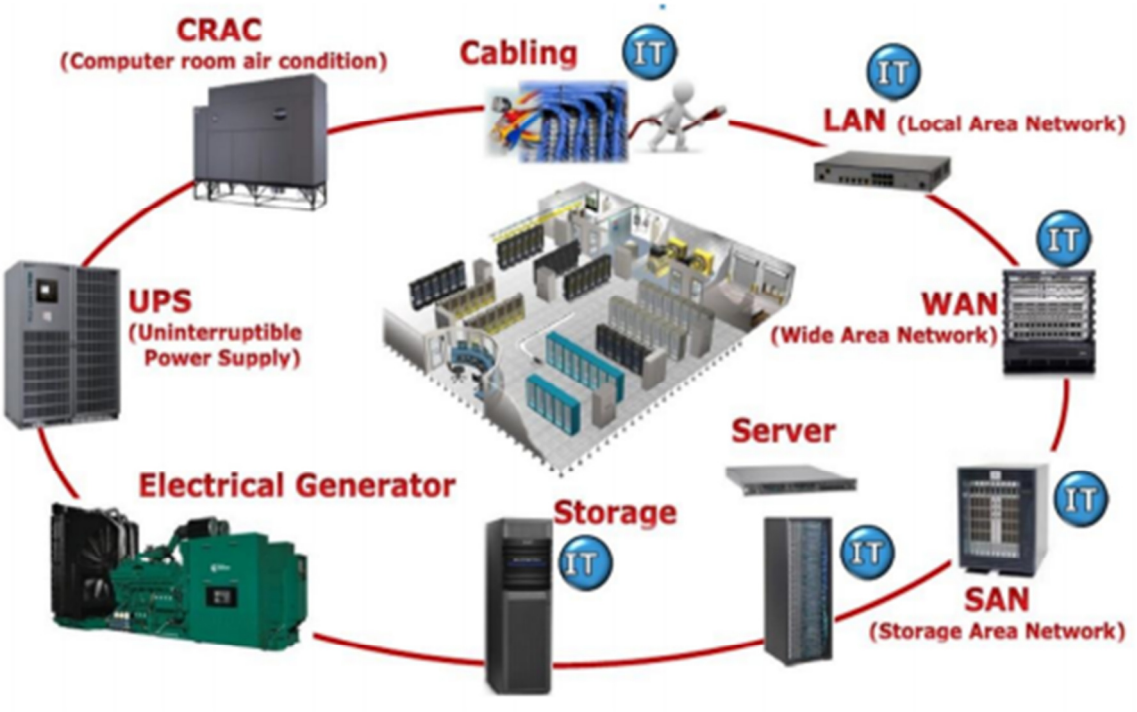
Najbolja strategija za oporavak od katastrofe u IT području opisana je razinom 7 prema klasifikaciji IBM-a i organizacije SHARE – potpuno automatizirano rješenje pri kojoj u slučaju katastrofe informacijski sustav automatski nastavlja raditi na vrućoj pričuvnoj lokaciji bez ikakvog prekida ili gubitka podataka.

Ukoliko se za izolirani informacijski sustav želi postići strategija oporavka od katastrofe opisana razinom 7, potrebno je sljedeće:

1. uspostaviti najmanje jednu vruću pričuvnu lokaciju s poslužiteljima, mrežnom opremom, uređajima za pohranu podataka te softverom koji su instalirani, u funkciji te imaju jednake funkcionalnosti kao informacijski sustav na primarnoj lokaciji,
2. uspostaviti mrežnu vezu visoke propusnosti između primarne i pričuvne lokacije korištenjem zakupljene linije, VPN veze preko Interneta ili čak privatnom optičkom vezom, ukoliko ju organizacija može izgraditi ili zakupiti,
3. uspostaviti izradu pričuvnih kopija podataka; strategija izrade kopije treba biti minimalno 3-2-1 što znači tri primjerka podataka (jedan u produkciji, dva u pričuvi), na dva medija (primjerice na dva različita uređaja za pohranu podataka) te na jednoj lokaciji izvan primarne tj. na pričuvnoj [**33**],
4. na primarnoj i na pričuvnoj lokaciji instalirati neko od softverskih rješenja za oporavak od katastrofe – neka od najpopularnijih su VMware SRM i NSX, Veeam Disaster Recovery Orchestrator, Veritas InfoScale ili Zerto Platform.

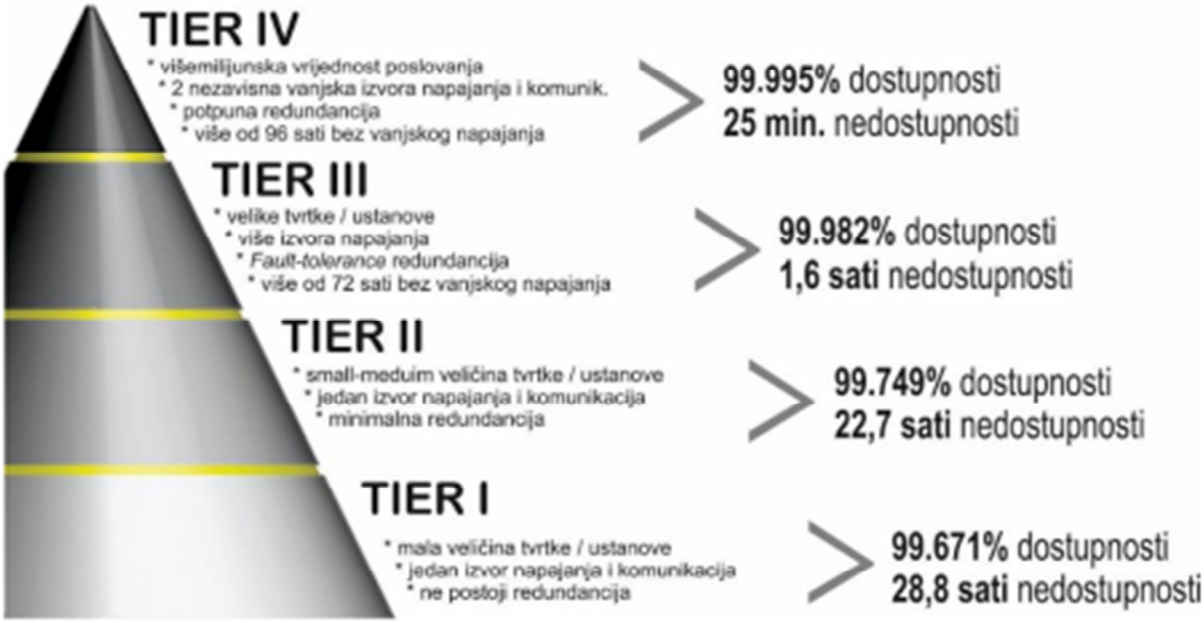
3.1. Podatkovni centar – ključni dio informacijskog sustava

Uobičajeno se glavni dijelovi IT infrastrukture nalaze u podatkovnom centru koji je u vlasništvu organizacije kojoj informacijski sustav pripada. Podatkovni centar predstavlja naziv za građevinu ili dio građevine sa posebno predviđenim prostorom za smještaj poslužiteljskih sustava te pripadajućih komponenti poput telekomunikacija i sustava za pohranu podataka. U pravilu sadrži redundantni sustav napajanja, telekomunikacijske priključke, klimatizaciju, sustav za nadzor ambijenta te samih uređaja (poslužitelji, aktivna mrežna oprema, uređaji za pohranu podataka) [**34**]. Dijelovi podatkovnog centra prikazani su na slici 21.



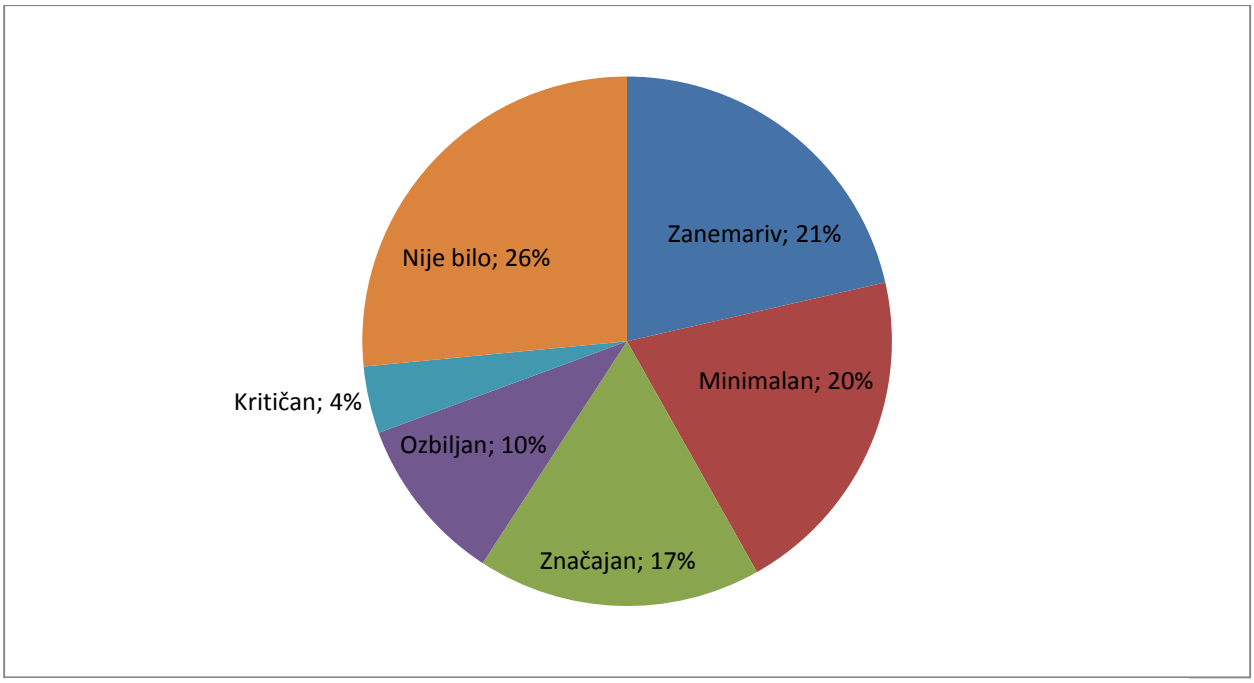
Slika 21 – Sastavni dijelovi podatkovnog centra [65]

Podatkovni centri projektiraju se sukladno standardima od kojih se najčešće primjenjuje TIA-942 (Telecommunications Industry Association) [**35**]. Taj standard sadrži preporuke koje se odnose na dizajn prostora namijenjenog za podatkovni centar, strukturno kabliranje, neprekidne izvore napajanja, klimatizaciju te ostale sastavnice. Sukladno tom standardu postoje 4 razine (engl. tier) podatkovnih centara s obzirom na dostupnost. Dostupnost predstavlja vjerojatnost da će podatkovni centar raditi na zadovoljavajući način u danom trenutku u vremenu. Računa se kao omjer prosječnog vremena do kvara (engl. mean time to failure, MTTF) i prosječnog vremena za oporavak (engl. mean time to repair, MTTR) prema formuli **Dostupnost = MTTF / (MTTF+MTTR)** [**36**]. Najbolji podatkovni centar (razina 4) može biti nedostupan do 25 minuta godišnje. U procjeni dostupnosti računa se da je u godini koja ima ukupno 525600 minuta nastupio jedan kvar od 25 minuta. Njegova dostupnost je 525600/(525600+25)=0,99995 ili **99,995%.** Podatkovni centar najniže kvalitete (razina 1) može biti nedostupan do 28,8 sati ili 1728 minuta godišnje. Sukladno primjeru za razinu 4, njegova dostupnost je tada 525600/(525600+1728)=0,99671 ili **99,671%**. Usporedba razina podatkovnog centra s odgovarajućim dostupnostima prikazana je na slici 22.

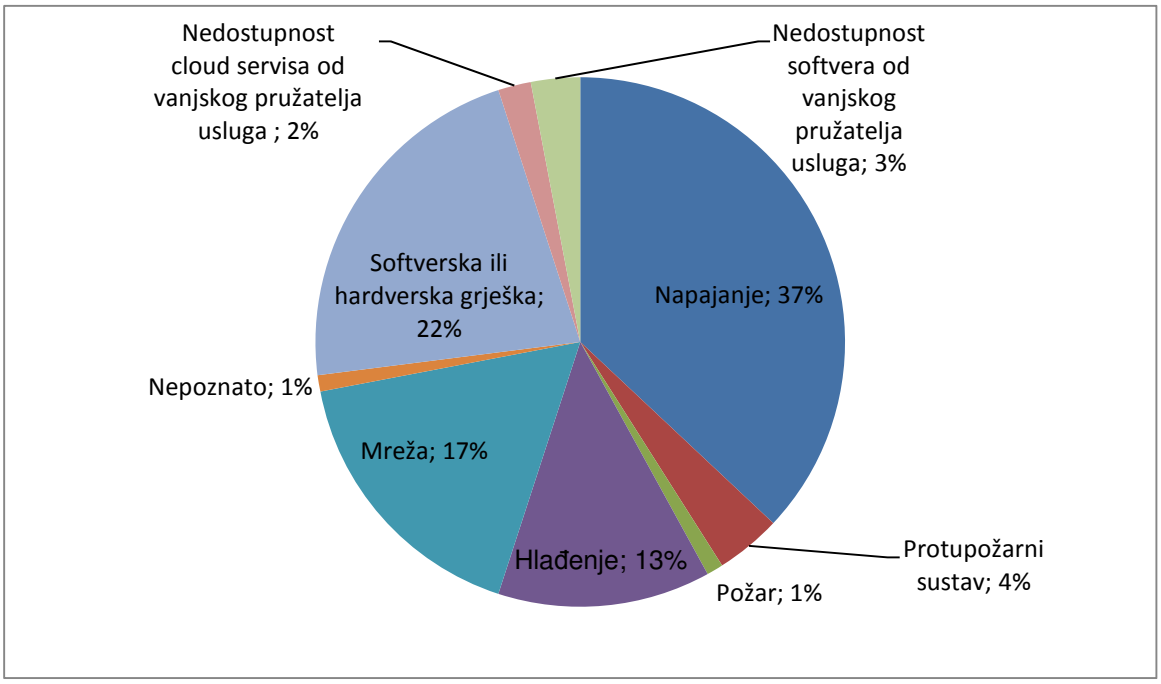


Slika 22 – Klasifikacija razina podatkovnog centra [66**]**

U ekstremnim slučajevima koji su rijetki, prekidi u radu podatkovnih centara uzrokovani su prirodnim katastrofama poput potresa, uragana, poplave. U godišnjem izvješću za 2020. godinu koje provodi organizacija Uptime Institute koja se bavi poboljšanjem učinkovitosti i pouzdanosti kritične poslovne infrastrukture utvrđeno je kako je 31% od preko 400 ispitanih kompanija imalo prekide u radu značajne, ozbiljne ili kritične razine (prikazano na slici 23). Većina ispitanih kompanija (njih 75%) priznalo je kako su se ti prekidi mogli izbjeći primjenom boljih organizacijskih ili upravljačkih procesa i politika. Kako je prikazano na slici 24, prekidi su uglavnom bili uzrokovani problemima s napajanjem i mrežom te greškama na hardveru i aplikacijama [**37**].

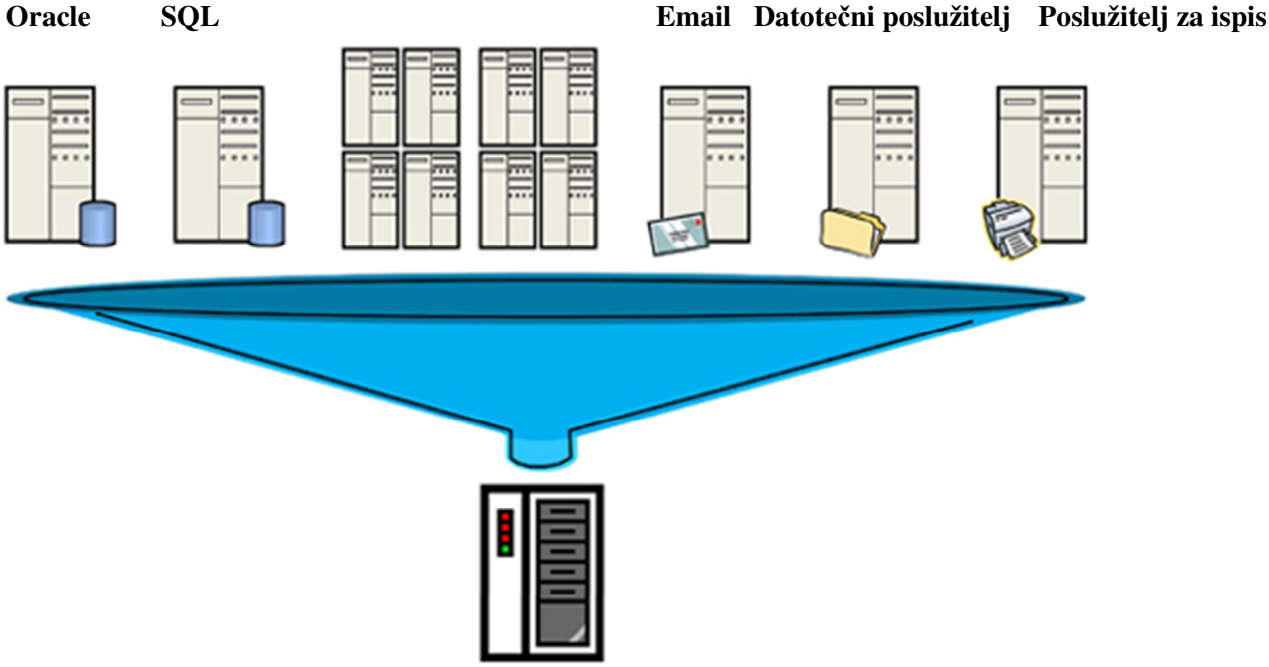


Slika 23 – Klasifikacija težine najznačajnijeg prekida u radu podatkovnog centra u razdoblju 2017 – 2020, N=494 [37]



Slika 24 – Uzroci posljednjeg značajnog prekida u radu, N=152 [37]

Suvremeni podatkovni centri temelje se na virtualizacijskoj infrastrukturi. Virtualizirati je moguće poslužitelje, mreže, uređaje za pohranu podataka te upravljački softver. Američka tvrtka VMware koja je tržišni predvodnik u području virtualizacije i servisa u oblaku u svojem proizvodu, odnosno rješenju naziva **softverski definirani podatkovni centar** (engl. **Software-Defined Datacenter, SDDC**) uključuje sva četiri navedena područja virtualizacije kao cjeloviti sustav.



Slika 25 – Virtualizacija poslužitelja [67]

Virtualizacija poslužitelja prikazana na slici 25 je tehnologija kojom se na jednom fizičkom poslužitelju pokreće više softverski izoliranih virtualnih poslužitelja. Na samostalnim fizičkim poslužiteljima rijetko se koristi više od 15% resursa. Virtualizacijom se određena aplikacija zajedno s operativnim sustavom enkapsulira u softverski spremnik naziva virtualni poslužitelj. Taj virtualni poslužitelj koristi određeni segment ukupnih memorijskih i procesorskih resursa fizičkog poslužitelja. Na taj način postiže se puno bolja iskoristivost budući da je na jednom fizičkom poslužitelju instalirano više takvih virtualnih koji koriste puno veću količinu raspoloživih resursa. Instalacija virtualnih poslužitelja mnogo je jednostavnija i brža od instalacije fizičkih. Korištenjem takvih poslužitelja mnogo je lakše ostvariti visoku dostupnost (HA) i neprekidnost rada.

Virtualizacija mreža je tehnologija koja razdvaja upravljanje mrežnim uređajima s mrežnim funkcijama odnosno s prosljeđivanjem mrežnog prometa. Na taj način postiže se bolje upravljanje mrežnim resursima i prometom te usklađenost sigurnosnih funkcija sa potrebama softvera koji koristi mrežu.

Virtualizacija uređaja za pohranu podataka omogućuje aplikacijama korištenje točno onoliko mrežnog prostora koliko im treba. Tom tehnologijom pojednostavljuje se upravljanje podatkovnim hardverom te korištenje sigurnosnih funkcija poput deduplikacije i replikacije podataka.

U SDDC rješenju na sve navedene virtualizacijske tehnologije nadograđuje se centralizirani upravljački softver kojim se s jednog mjesta upravlja svim virtualizacijskim resursima [**38**].

SDDC rješenje podatkovnog centra ima nekoliko prednosti u odnosu na klasični podatkovni centar [**39**]:

1. jednostavnije upravljanje – centralizirani virtualni upravljački softver omogućuje upravljanje hardverskim i softverskim resursima podatkovnog centra s jednog mjesta,
2. fleksibilnost – SDDC omogućuje jednostavnu prilagodbu na povećanje zahtjeva za hardverskim i softverskim resursima,
3. pouzdanost – u slučaju kvara hardverskog uređaja u podatkovnom centru resursi se automatski preraspoređuju na drugi, funkcionalan uređaj,
4. optimizacija korištenja resursa – centralizirani virtualni upravljački softver ima analitičke alate koji prikupljaju podatke o korištenju resursa što olakšava planiranje i organiziranje sustava u cilju njegova efikasnijeg korištenja.

Ovakvo rješenje može se primijeniti u privatnom okruženju (vlastitom podatkovnom centru) ili na uslugama u oblaku vanjskih dobavljača. Što se tiče oporavka od katastrofe, SDDC omogućuje jednostavan prijelaz na pričuvnu lokaciju budući da nije potrebna rekonfiguracija mreže, diskovnog prostora ili poslužitelja kako bi aplikacije nastavile raditi. Cjelokupna procedura prelaska na pričuvnu lokaciju može biti automatizirana, a jedino što se unaprijed treba definirati je RTO za pojedine aplikacije [**40**].

Primarni i pričuvni podatkovni centar u izoliranom informacijskom sustavu uobičajeno su povezani kroz mrežu širokog područja (engl. Wide Area Network, WAN). Mogućnosti povezivanja su različite. Od pružatelja usluga moguće je zakupiti mrežnu vezu tipa MetroEthernet, Frame Relay, IP/MPLS, optičku vezu ili virtualnu privatnu mrežu (engl.

Virtual Private Network - VPN) korištenjem Interneta. Ali, u svakom slučaju, ukoliko se u izoliranom informacijskom sustavu nalaze klasificirani podatci, krajnje točke mrežnih lokacija sustava trebaju biti štićene odgovarajućim hardverskim sigurnosnim uređajem, vatrozidom ili kripto uređajem. Kripto uređaji su relativno kompliciranizaodržavanje buduće da je za njihovo korištenje potrebno imati mogućnost kreiranja i upravljanja kripto ključevima, ali predstavljaju najpouzdanije rješenje za postizanje sigurnosti mrežnih veza. Njima se postiže da je sav promet između dva usmjerivača odnosno lokacije kriptiran te ga potencijalni napadač ne može preslušavati ili koristiti kao točku upada u sustav [**41**]. Zavod za sigurnost informacijskih sustava kao središnje državno tijelo u Republici Hrvatskoj čija je funkcija obavljanje poslova u tehničkim područjima informacijske sigurnosti državnih tijela propisao je registar odobrenih kriptografskih uređaja za zaštitu linijskog prometa, IP prometa te VPN veza. U njemu su navedeni uređaji koji osiguravaju stupnjeve tajnosti od OGRANIČENO do VRLO TAJNO. Za stupanj tajnosti OGRANIČENO dovoljan je komercijalni vatrozid Cisco ASA 5510/5520/5540 Series, a za više stupnjeve tajnosti potrebno je imati kripto uređaj specijaliziranih proizvođača kao što je SINA, Rohde & Schwarz ili Thales [**42**].

4. Rješenje za oporavak od katastrofe na izoliranom informacijskom sustavu

Kako je navedeno, sukladno razini 7 prema klasifikaciji IBM-a i organizacije SHARE najbolje rješenje za oporavak od katastrofe na primarnoj lokaciji (podatkovnom centru) podrazumijeva automatski nastavak rada na vrućoj pričuvnoj lokaciji bez prekida ili gubitka podataka. Tradicionalna rješenja za oporavak od katastrofe imaju nedostatke jer ne podržavaju automatizaciju i fleksibilnost nego je većinu aktivnosti potrebno odraditi ručno. Ukoliko se postupak oporavka želi automatizirati potrebno je osigurati sljedeće [**43**]:

1. oporavak aplikacijskih poslužitelja s istim IP adresama kao na primarnoj lokaciji – ovo je važno zato su IP adrese povezane sa sigurnosnim postavkama, uravnoteživačem opterećenja (engl. load balancer), DNS postavkama, aplikacijskim međuzavisnostima,
2. osiguranje istih sigurnosnih postavki na aplikaciji kao što su na primarnoj lokaciji – tradicionalna rješenja temelje se na ručnim podešavanjima i sinkroniziranjem sigurnosnih postavki između primarne i pričuvne lokacije što uzima puno vremena, a moguće su i greške.

Zbog toga u svrhu postizanja razine 7 oporavka od katastrofe (potpuna automatizacija) na izoliranom informacijskom sustavu potrebno je koristiti profesionalno rješenje. Jedno od kvalitetnih rješenja te vrste je **VMware NSX** u kombinaciji s **VMware Site Recovery Manager (SRM)** [**44**].

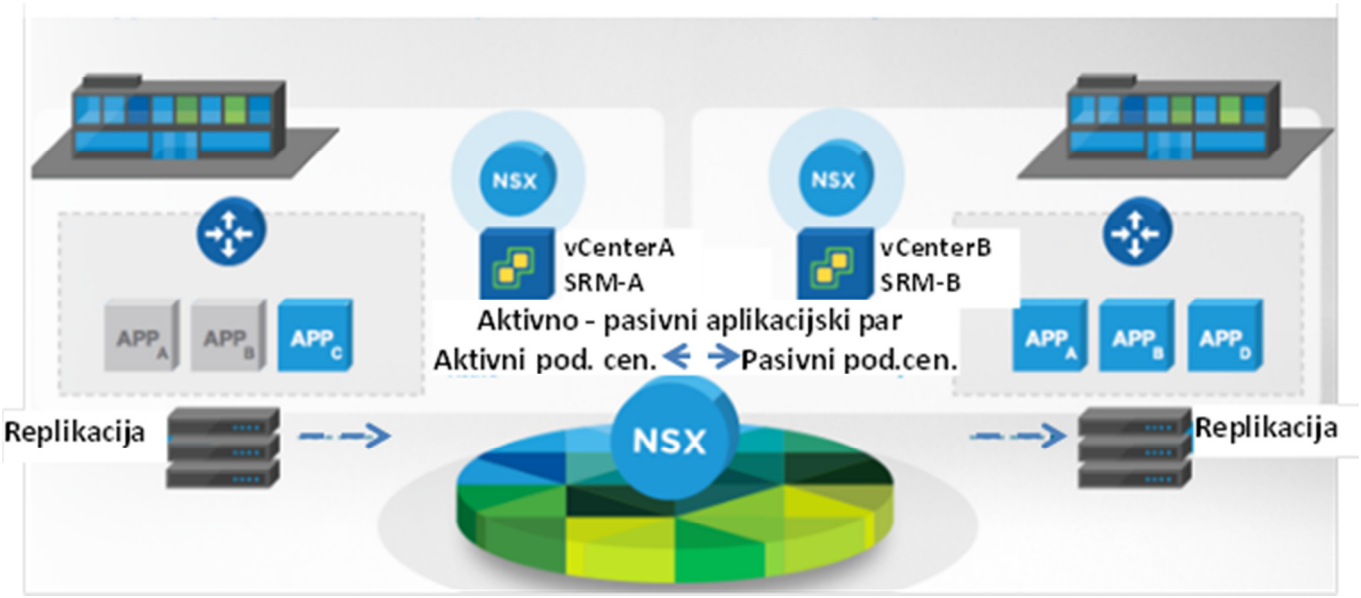
VMware NSX je virtualizacijska platforma koja odvaja mrežne servise od mrežne fizičke infrastrukture. Ona sadrži kolekciju logičkih mrežnih servisa poput logičkih prespojnika, logičkih usmjerivača, logičkih vatrozida, logičkih VPN konekcija i distribuiranih sigurnosnih funkcija. Na taj način jednostavno je kreirati, modificirati, brisati i raditi sigurnosne kopije virtualne mrežne infrastrukture. Primjena te virtualizacijske platforme podrazumijeva korištenje softverski definiranog podatkovnog centra na obje lokacije, primarnoj i pričuvnoj. Pri tome obje lokacije koriste istu logičku mrežu, a konfiguracije se mogu jednostavno seliti s jedne na drugu. Takvim pristupom koji se temelji na softveru, a ne na hardveru, rješavaju se problemi iz područja sigurnosni, automatizacije te kontinuiteta rada aplikacija.

VMware SRM je rješenje za upravljanje kontinuitetom poslovanja i oporavak od katastrofe kojim se može planirati, testirati i pokretati oporavak virtualnih poslužitelja s primarne na pričuvnu lokaciju i obrnuto. U slučaju potpunog ispada primarne lokacije, SRM će temeljem unaprijed definiranog plana oporavka pokrenuti virtualne poslužitelje na pričuvnoj lokaciji s repliciranog diskovnog prostora. Plan oporavka definira redoslijed uključivanja virtualnih poslužitelja te mrežne i sigurnosne postavke koje se na njima moraju primijeniti.

Informacijski sustav koji je instaliran u dva ili više povezanih podatkovnih centara može koristiti jedan kao primarni, a drugi odnosno ostale kao pričuvne (aktivno/pasivna implementacija prikazana na slici 26) ili ih može sve koristiti kao aktivne (aktivno/aktivna implementacija prikazana na slici 27).

U slučaju pasivne implementacije aplikacija A je aktivna na primarnoj lokaciji, a u slučaju katastrofe virtualni poslužitelj koji ju izvršava pokreće se na pričuvnoj lokaciji koja se u uobičajenim okolnostima ne koristi. U idealnom slučaju pričuvna lokacija nalazi se u drugom potresnom području, a opet dovoljno blizu da nema velikog efekta latencije podataka.

U drugom slučaju oba podatkovna centra aktivna su cijelo vrijeme. Mrežna infrastruktura uvezana je na logičkoj razini čime se omogućuje da se hardver na različitim lokacijama može udružiti u jedan objedinjeni komplet IT resursa čime se postiže njihovo optimalno korištenje. Dio aplikacija stalno je pokrenut na prvoj, a dio na drugoj odnosno ostalim lokacijama [**45**].



Slika 26 – Aktivno/pasivna VMware NSX i SRM implementacija primarnog i pričuvnog podatkovnog centra [68]

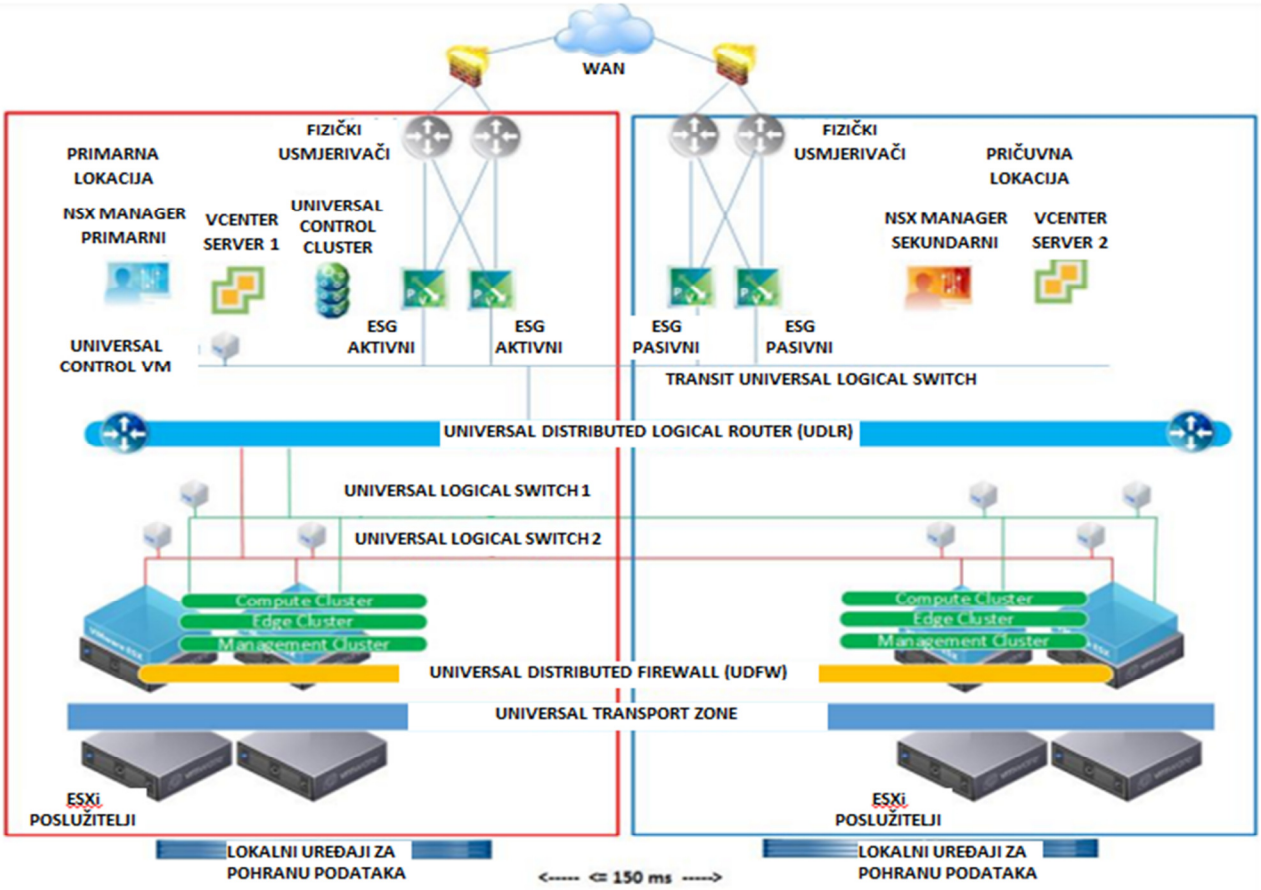
Slika 27 – Aktivno/aktivna VMware NSX implementacija primarnog i pričuvnog podatkovnog centra [68]

4.1. Komponente rješenjaVMware NSX i SRM

VMware vSphere je virtualizacijska platforma koja se temelji na fizičkom poslužitelju **ESXi** te na poslužiteljskoj aplikaciji **vCenter Server.** ESXi je fizički poslužitelj na kojem je instaliran tip 1 hipervizor. To je, u osnovi, operativni sustav koji se izvodi izravno na hardveru glavnog računala i obavlja kontrolu njegovih hardverskih resursa te upravljanje gostujućim operativnim sustavima ili virtualnim poslužiteljima koji su instalirani na njemu [**46**]. vCenter Server je poslužiteljska aplikacija koja upravlja ESXi poslužiteljima kao i virtualnim poslužiteljima koji se nalaze na njima. ESXi poslužitelji u jednom podatkovnom centru koriste zajednički diskovni prostor na uređajima za pohranu podataka (engl. **local storage**).

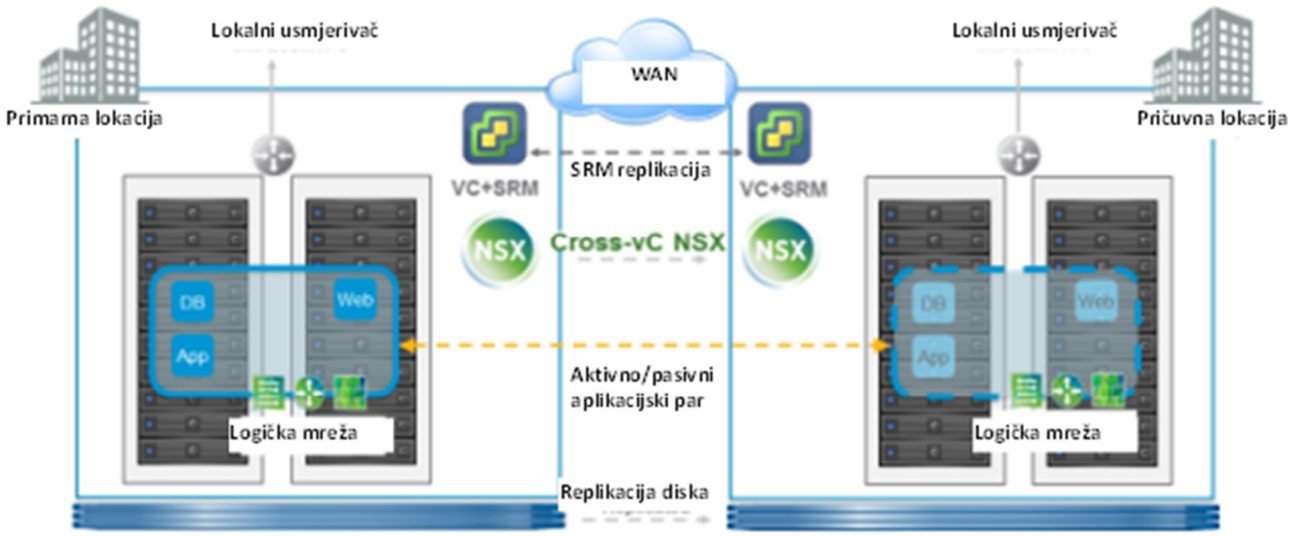
VMware NSX rješenje pretpostavlja korištenje najmanje dva podatkovna centra. Takva primjena naziva se **Cross-vC (Virtual Center) NSX.** ESXi poslužitelji u svakome podatkovnom centru podijeljeni su u **grupe** (engl. **cluster**). U **upravljačkoj grupi** (engl. **management cluster**) nalaze se ESXi poslužitelji na kojima su instalirani upravljački virtualni poslužitelji – **vCenter Server, NSX Manager, NSX Controller.** Osim te postoje još **rubna** i **računska grupa** (engl. **edge** and **compute cluster**) u kojima se nalaze ESXi poslužitelji na kojima su pokrenuti ostali (aplikacijski i korisnički) virtualni poslužitelji [**47**]. Svaki podatkovni centar ima svoju **vCenter Server domenu** u kojoj se nalazi najmanje jedan

vCenter Server koji upravlja ESXi poslužiteljima iz svih navedenih grupa. **Lokalni objekti** sadržani su unutar jedne vCenter Server instance (domene). Ti objekti imaju oznaku **global** u NSX upravljačkom sučelju (engl. **NSX UI**). **Univerzalni objekti** imaju raspon u više vCenter Server domena i imaju oznaku **universal** u NSX UI. **Primarni NSX Manager** je virtualni poslužitelj koji kreira i upravlja univerzalnim objektima. U NSX okruženju može postojati samo jedan primarni manager. **Sekundarni NSX Manager** ne može kreirati univerzalne objekte, ali je u stalnoj sinkronizaciji s primarnim što znači da se objekti koji su kreirani na primarnom automatski preslikavaju na sekundarni. U NSX okruženju može postojati maksimalno sedam sekundarnih NSX manager što bi značilo da informacijski sustav u idealnom slučaju može imati jedan primarni podatkovni centar i sedam pričuvnih. **Universal Synchronization Service (USS)** je servis koji replicira univerzalne objekte s primarnog na sekundarne NSX managere. **Universal Control Cluster (UCC)** sadrži informacije o globalnim i univerzalnim objektima. **Universal Transport Zone (UTZ)** predstavlja skup univerzalnih logičkih objekata koji su raspoređeni kroz grupe (clustere) na svim lokacijama. Ukoliko se želi da resursi određenog ESXi poslužitelja budu raspoređeni u više vCenter Server domena, grupa u kojoj se nalazi mora biti ubačena u UTZ. **Universal Logical Switch (ULS)** je mrežni prespojnik koji je smješten u UTZ čime je dostupan u svim vCenter Server domenama. To je logički uređaj koji omogućuje povezivost po podatkovnom (drugom) sloju OSI modela u različitim vCenter Server domenama odnosno u različitim podatkovnim centrima. **Universal Distributed Logical Router (UDLR)** je mrežni usmjerivač koji je smješten u UTZ čime je dostupan u svim vCenter Server domenama. On omogućuje povezivost po mrežnom sloju u različitim vCenter Server domenama odnosno u različitim podatkovnim centrima. To je logički uređaj koji omogućuje da se određena IP adresa ili adresni raspon može seliti iz jednog u drugi podatkovni centar. **Universal Distributed Firewall (UDFW)** je vatrozid koji je smješten u UTZ čime je dostupan u svim vCenter Server domenama. Ovaj logički uređaj omogućuje da se u svim vCenter Server domenama primjenjuje ista sigurnosna politika. **Edge Services Gateway (ESG)** je logički uređaj koji je također smješten u UTZ i pruža mrežne usluge poput DHCP, VPN, NAT, uravnoteživač opterećenja u svim vCenter Server domenama. **Local Egress** odnosno lokalni izlaz upravlja mrežnim rutama koje su dostupne ESXi poslužiteljima na pojedinoj lokaciji odnosno vCenter Server domeni. UCC uči mrežne rute od pojedinih domena i distribuira ih ESXi poslužiteljima. Njima je točno definirano kojim fizičkim mrežnim usmjerivačima će ići mrežni promet [**45**]. Primjena Cross-vC NSX rješenja prikazana je na slici 28.



Slika 28 – Primjena Cross-vC NSX rješenja na primarnoj i pričuvnoj lokaciji [45]

VMware SRM je na svakoj lokaciji integriran s vCenter Serverom i s VMware NSX-om. On upravlja replikacijom diskovnog prostora na uređajima za pohranu podataka s jedne na drugu lokaciju te se brine za provedbu oporavka za situacije planirane i neplanirane nedostupnosti poslužitelja ili cijele lokacije. Primjena integriranog NSX i SRM rješenja prikazana je na slici



Slika 29 - Integrirano NSX i SRM rješenje na primarnoj i pričuvnoj lokaciji [48]

4.2. Scenariji primjene rješenja u svrhu oporavka od katastrofe

Preduvjeti za primjenu integriranog VMware NSX i SRM rješenja su sljedeći [**48**]:

1. Na obje lokacije (primarnoj i pričuvnoj) mora biti instalirano osnovno VMware okruženje – ESXi poslužitelji s vCenter Serverom,
2. Na obje lokacije instaliran je VMware SRM koji je integriran s vCenter Serverom i VMware NSX Managerom na toj lokaciji,
3. Diskovni prostor mora se replicirati s uređaja za pohranu podataka na primarnoj lokaciji na uređaje na pričuvnoj lokaciji; replikacija se može podesiti korištenjem alata koji su ugrađeni u uređaje za pohranu podataka ili korištenjem aplikacije **vSphere Replication Appliance** instalirane na obje lokacije,
4. NSX mora biti podešen na sljedeći način:
    a. na obje lokacije instaliran je NSX Manager; na primarnoj je glavni, a na pričuvnoj je sekundarni; na obje lokacije Manager je integriran s vCenter Serverom i VMware SRM-om,
    b. na obje lokacije podešena je Cross-vC varijanta rješenja koja uključuje:
        - Universal Logical Switch (ULS), Universal Distributed Logical Router (UDLR), Universal Distributed Firewall (UDFW) – ovime se postiže da se na obje lokacije nalazi ista logička mreža na podatkovnom (2) i mrežnom (3) sloju te ista sigurnosna politika,
        - na NSX Manageru na primarnoj lokaciji kreiran je Universal Control Cluster (UCC) koji upravlja svim univerzalnim i globalnim objektima,
        - aktivan je Universal Syncronization Service koji replicira univerzalne objekte s primarnog vCenter Servera na onaj na pričuvnoj lokaciji,
        - UDLR upravlja Edge Services Gateway (ESG) logičkim uređajima na obje lokacije čime upravlja lokalnim mrežnim prometom i mrežnim uslugama na svakoj od njih,
        - u slučaju ispada glavnog NSX Managera i gubitka UCC-a sekundarni NSX Manager preuzima ulogu glavnog i rekreira UCC bez gubitka konfiguracijskih podataka.

Predviđena su tri scenarija uporabe, oporavak dijela aplikacije (engl. Partial Application Failover), oporavak cijele aplikacije (engl. Full Application Failover) i oporavak cijele lokacije (engl. Site Failover) [**48**].

Oporavak dijela aplikacije – ovaj slučaj pojavljuje se kod višerazinskih aplikacija koje koriste zasebne poslužitelje za web, bazu podataka i samu aplikaciju. Kada jedan od tih poslužitelja, primjerice web, postane nedostupan na primarnoj, automatski se pokreće na pričuvnoj lokaciji dok ostala dva poslužitelja i dalje rade na primarnoj lokaciji. To se postiže Cross-vC implementacijom NSX-a zbog koje se na obje lokacije nalazi ista logička mreža s istim IP adresnim rasponom i sigurnosnim postavkama. Zbog toga web poslužitelj koji se pokreće na pričuvnoj lokaciji ima istu IP adresu kao i originalni koji se nalazi na primarnoj lokaciji. Oporavak odnosno pokretanje poslužitelja na pričuvnoj lokaciji provodi se automatski pa korisnici informacijskog sustava u pravilu i ne primjećuju da je originalni poslužitelj postao nedostupan.

Oporavak cijele aplikacije – u ovom slučaju sve komponente višerazinske aplikacije odnosno web poslužitelj, poslužitelj baza podataka i aplikacijski poslužitelj postaju nedostupni na primarnoj lokaciji i automatski se pokreću na pričuvnoj lokaciji. Sav mrežni promet koji se odnosi na te poslužitelje automatski se preusmjerava na pričuvnu lokaciju te korisnici opet ne primjećuju prekid u radu. Jedino što se s korisničke strane eventualno može uočiti je malo sporiji pristup na servise poslužitelja zbog mrežne latencije između njihovih korisničkih računala koja se nalaze na primarnoj lokaciji prema poslužiteljima koji se sada nalaze na pričuvnoj lokaciji.

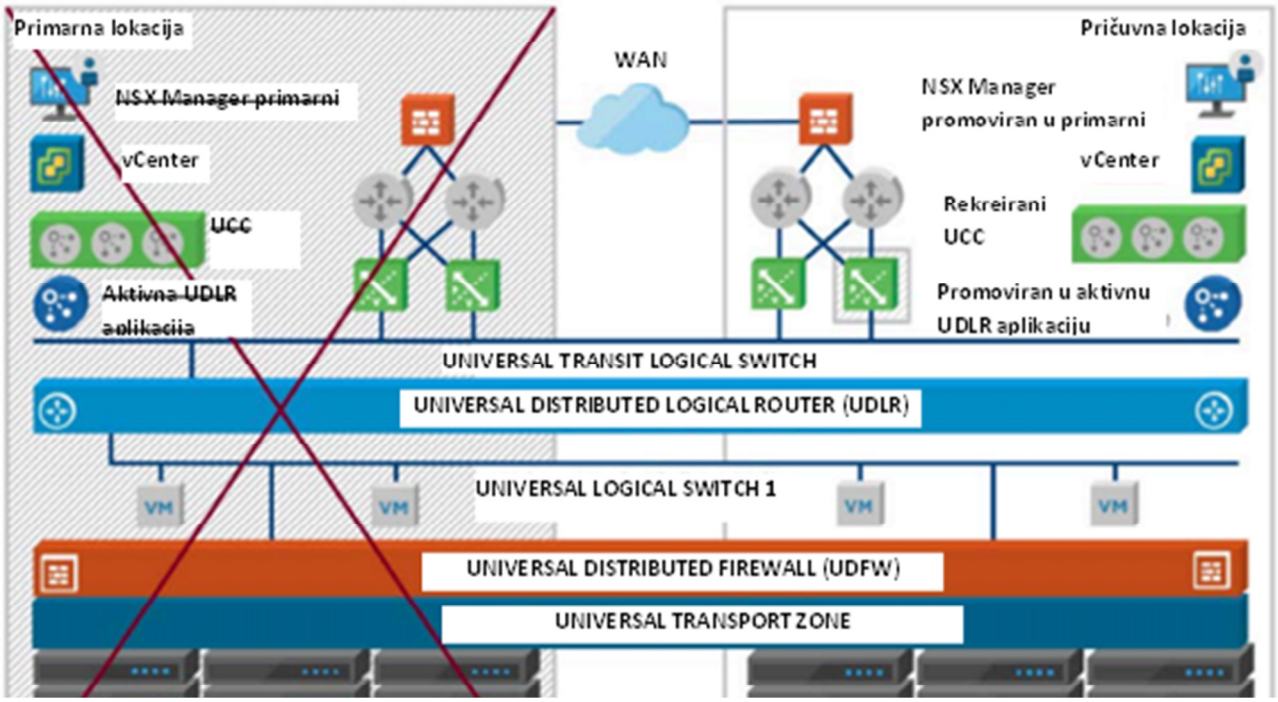
Oporavak cijele lokacije [**49**] – u situacijama koje se mogu okarakterizirati kao katastrofa, primjerice kad nestane napajanja na primarnoj lokaciji te se tamo isključe svi ESXi poslužitelji, uređaji za pohranu podataka te mrežni uređaji, cjelokupni informacijski sustav nastavit će raditi na pričuvnoj lokaciji. U takvoj situaciji VMware NSX i SRM automatski će odraditi sljedeće:

1. SRM će pokušati izvršiti sinkronizaciju uređaja za pohranu podataka na pričuvnoj s onim na primarnoj lokaciji;
2. SRM će pokušati isključiti poslužitelje na primarnoj lokaciji; neovisno o tome hoće li ih uspjeti isključiti, uključit će se njihove kopije na pričuvnoj lokaciji; stanje u kojem će se nalaziti aplikacije i podatci na kopijama poslužitelja ovisi o posljednjoj

sinkronizaciji s uređaja za pohranu podataka na primarnoj na takav uređaj na pričuvnoj lokaciji;

3. NSX će promovirati sekundarni NSX manager koji se nalazi na pričuvnoj lokaciji u primarni;
4. NSX će rekreirati Universal Control Cluster na sekundarnoj lokaciji; time će logičke mrežne i sigurnosne komponente NSX rješenja (ULS, UDLR, UDFW) biti i dalje dostupne zbog čega će poslužitelji moći koristiti mrežne postavke s primarne lokacije;
5. nakon što primarna lokacija opet postane dostupna, SRM će sinkronizirati uređaj za pohranu podataka na toj lokaciji s onim na pričuvnoj;
6. SRM će sinkronizirati kopije poslužitelja na pričuvnoj lokaciji s izvornim poslužiteljima na primarnoj lokaciji;
7. SRM će započeti slijedno isključivati kopije poslužitelja na pričuvnoj lokaciji i uključivati odgovarajuće poslužitelje na primarnoj lokaciji;
8. NSX će aktivirati primarni NSX manager na primarnoj lokaciji, a onaj na sekundarnoj spustiti na razinu sekundarnog,
9. NSX će rekreirati Universal Control Cluster na primarnoj lokaciji.

Shema oporavka cijele lokacije prikazana je na slici 30.



Slika 30 – Oporavak cijele lokacije [44]

U svakom slučaju, kako bi gubitak podataka (RPO) bio što manji u SRM-u je važno kvalitetno podesiti parametre replikacije diskovnih prostora s primarne na pričuvnu lokaciju. Ako se ona izvršava jako često, prilikom ispada primarne lokacije kopije poslužitelja na pričuvnoj lokaciji sadržavat će gotovo u potpunosti aktualne podatke.

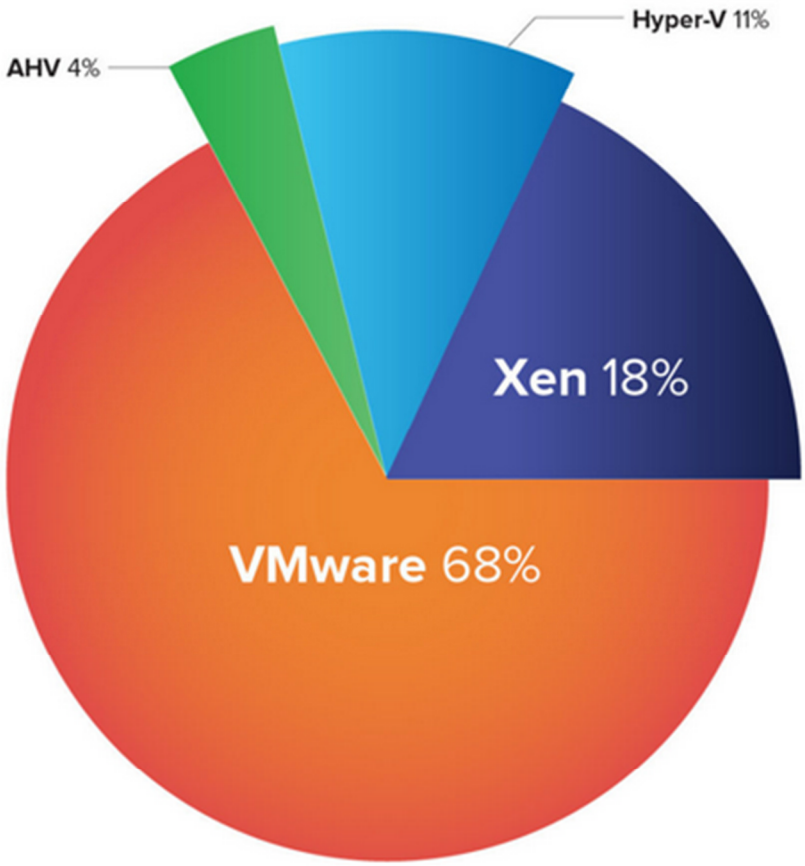
U svrhu povećanja sigurnosti cjelokupnog rješenja potrebno je implementirati procedure izrade pričuvnih kopija podataka za ključne elemente [**44**]:

1. VMware NSX – sistemske konfiguracije te dnevnički zapisi trebaju se pohranjivati na udaljenu lokaciju koja je dostupna NSX Managerima na obje lokacije, primarnoj i pričuvnoj. Pričuvna kopija nije velika jer ne sadrži cjelokupni virtualni poslužitelj. Kopija virtualnog poslužitelja nalazi se na pričuvnoj lokaciji u obliku sekundarnog NSX Managera. U slučaju katastrofe, kad primarna lokacija postane nedostupna, sekundarni NSX Manager preuzima ulogu primarnog, povlači podatke iz pričuvne kopije i aktivira sve logičke mrežne i sigurnosne NSX komponente (ULS, UDLR, UDFW),
2. vCenter Server je virtualni poslužitelj te se za njega kao i za bilo koji drugi virtualni poslužitelj trebaju izrađivati pričuvne kopije korištenjem njegovih ugrađenih sigurnosnih funkcija ili korištenjem specijaliziranog alata za njihovu izradu poput Veeam Backup & Replication,
3. VMware SRM sadrži bazu podataka koja se treba pohranjivati na udaljenoj lokaciji kako bi bila dostupna u slučaju ispada na primarnoj lokaciji. Slično kao i NSX, i SRM ima sekundarnu instalaciju na pričuvnoj lokaciji. S obzirom da je SRM instaliran na virtualnom poslužitelju, trebaju se izrađivati njegove pune pričuvne kopije korištenjem specijaliziranog alata.

4.3. Ocjena rješenja VMware NSX i SRM

VMware NSX kao platforma jedno je od najpopularnijih virtualizacijskih rješenja za softverski definirane podatkovne centre. VMware SRM također je popularno rješenje za upravljanje dostupnošću aplikacija u privatnom oblaku ili u informacijskim sustavima koji imaju dva ili više podatkovnih centara. Ocjene kvaliteta tih rješenja na relevantnim portalima za ocjenjivanje kvalitete softvera su 3,9/5 za NSX [**50**] i 4,1/5 za SRM [**51**].

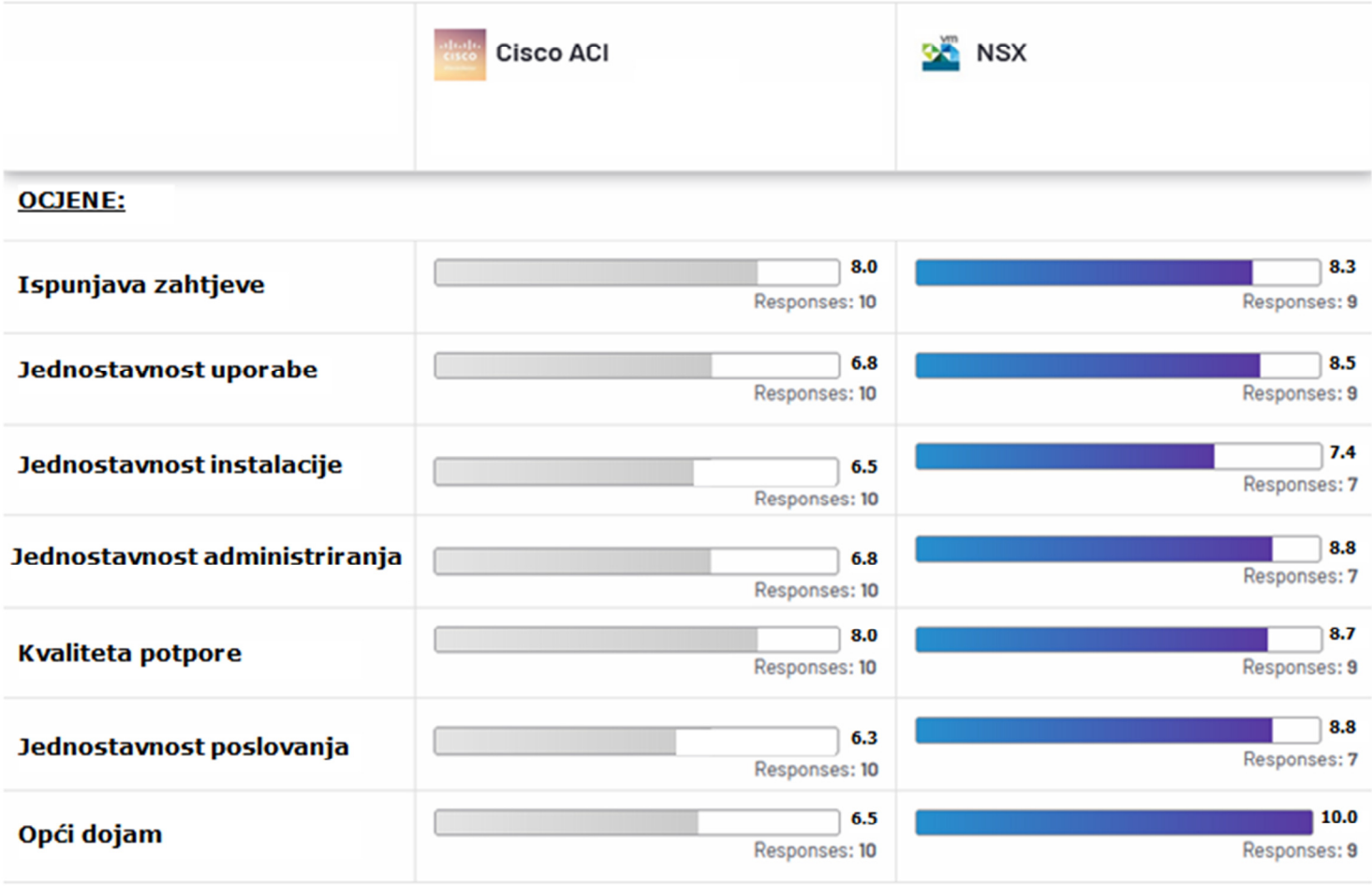
Navedena rješenja koriste se u okruženju koje koristi ESXi fizičke poslužitelje na kojima je instaliran vCenter Server koji upravlja njima te virtualnim poslužiteljima. Općenito je **VMware vSphere** uz **Citrix XenServer**, **Microsoft Hyper-V** i **Nutanix AHV** jedna od četiri najveće kompanije na tržištu virtualizacijskih tehnologija. Prema jednoj analizi tržišta provedenoj krajem 2018. g. na 758 poslovnih organizacija u SAD-u i prikazanoj na slici 31, VMware dominira budući da ga koristi ukupno 68% anketiranih organizacija [**52**].



Slika 31 - Udio virtualizacijskih tehnologija u organizacijama, N=758 [52]

VMware vSphere je profesionalno rješenje za virtualizaciju podesno za cjelokupan raspon korisnika, od malih poduzeća do korporacija. Njegove prednosti su to što podržava korištenje velikog broja fizičkih ESXi poslužitelja, virtualizaciju Windows i Linux operativnih sustava, migraciju fizičkih poslužitelja u virtualne, uravnoteživanje opterećenja, migraciju virtualnih poslužitelja u slučaju kvara fizičkog te integraciju s privatnim i javnim oblakom [**53**].

Što se tiče VMware NSX-a kao rješenja u području softverski definiranih podatkovnih centara usporedivi profesionalni softverski alati su **Cisco ACI**, **Juniper Contrail** i **Arista Networks** [**54**]. Od navedenih tvrtki najveći tržišni udio u tom području imaju VMware i Cisco. Iz tog razloga velike organizacije sa složenim informacijskim sustavima često koriste VMware NSX i SRM ili Cisco ACI. Odabir jednog ili drugog rješenja ovisi o specifičnostima informacijskog sustava pojedine organizacije te o cijeni koja je opet ovisna o tehničkim specifikacijama sustava. Većina recenzija daje usporedive rezultate za ta dva rješenja kako je prikazano na slici 32 [**55**].



Slika 32 - Usporedba Cisco ACI i VMware NSX rješenja [55]

Bitne funkcionalnosti koje nudi NSX kao rješenje su [**56**]:

1. mikrosegmentacija i spuštanje sigurnosti na razinu individualnih komponenti sustava,
2. efikasno korištenje mrežnih resursa zbog automatizacije,
3. mobilnost radnog opterećenja unutar i između podatkovnih centara, neovisno o fizičkoj topologiji mreže,
4. integracija s platformama za upravljanje okruženjem oblaka,
5. integracija s VMware rješenjima za analizu dnevničkih zapisa i otklanjanje problema,
6. upravljanje sigurnošću na razini IP i MAC adresa, ali i temeljem vrste operativnog sustava te informacijama vezanim uz pojedinu aplikaciju,
7. seljenje mrežnih i sigurnosnih postavki izvan granica podatkovnog centra.

U recenzijama stručnih korisnika navedeni su sljedeći prijedlozi za nadogradnju VMware NSX-a [**57**]:

1. bilo bi dobro ubaciti mogućnost inspekcije ESXi poslužitelja u svrhu otkrivanja nekompatibilnosti s funkcionalnostima sustava,
2. NSX Manager trebao bi se moći registrirati izravno na vCenter Server – sada se registrira preko Transportnih zona što usložnjava administraciju,
3. treba povećati broj sigurnosnih grupa i pravila čime će se olakšati implementacija na složenijim informacijskim sustavima,
4. potrebno je poboljšati integracija s usmjerivačkim protokolom OSPF koji je jedan od najčešće korištenih usmjerivačkih protokola u WAN mrežama,
5. treba bolje razraditi funkcije praćenja (monitoring) za fizičke i virtualne poslužitelje.

Bitne funkcionalnosti koje nudi SRM kao rješenje su [**58**]:

1. mogućnost primjene na više podatkovnih centara, u privatnom ili javnom oblaku,
2. testiranje migracije poslužitelja sa zaštićene (primarne) na pričuvnu lokaciju te njihovog povratka na primarnu lokaciju,
3. automatizacija tijeka oporavka od katastrofe,
4. centralno upravljanje planovima oporavka od katastrofe,

U recenzijama stručnih korisnika navedeni su sljedeći prijedlozi za nadogradnju VMware SRM-a [**59**]:

1. replikacija bi trebala biti brža jer se ne uspijeva završiti na vrijeme ako poslužitelji imaju velike diskove,

2. dnevnički zapisi (engl. event log) trebaju biti detaljniji jer ne daju dovoljno podataka u svrhu rješavanja problema (engl. troubleshoot) prilikom problema s replikacijom i drugim operacijama,
3. vezano uz dnevničke zapise, trebalo bi implementirati mogućnost preciznog praćenja procesa replikacije,
4. upravljačka konzola treba biti preglednija za korištenje,
5. potrebna je bolja integracija s ostalim rješenjima za pohranu podataka.

Može se zaključiti kako se uporabom NSX-a sa SRM-om kao cjelovitim rješenjem za oporavak od katastrofe unutar informacijskog sustava organizacije ostvaruju višestruke koristi:

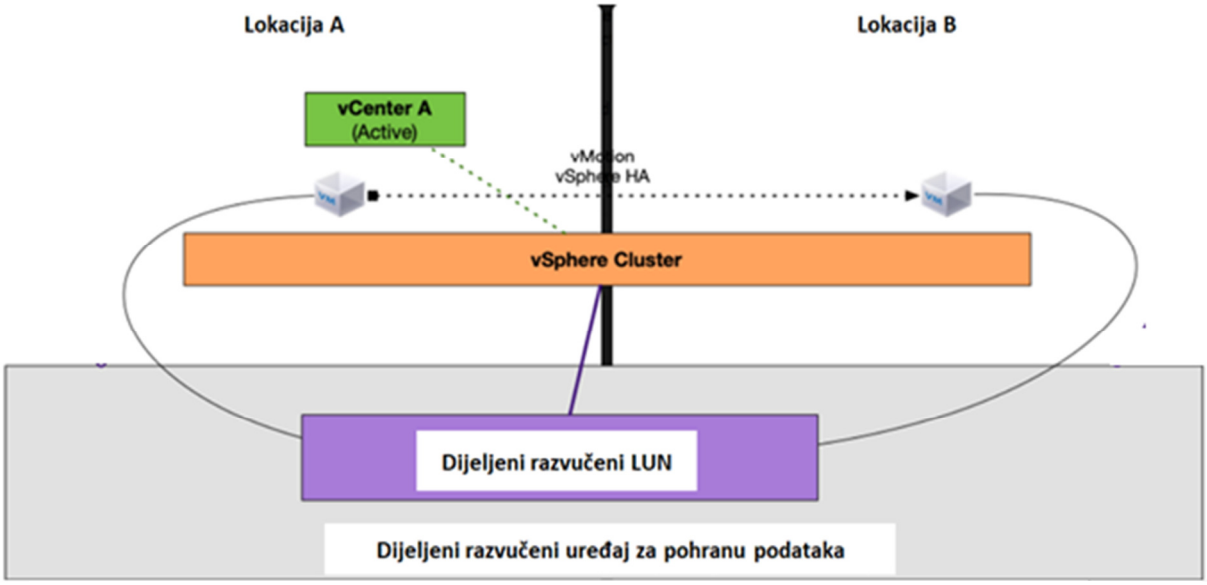
1. financijske uštede zbog smanjene potrebe za mrežnim prespojnicima, vatrozidovima te poslužiteljima,
2. uštede u radu administratora zbog olakšane administracije cjelokupnog VMware okruženja,
3. u slučaju katastrofe podatci i aplikacije sačuvani su na pričuvnoj lokaciji [**60**].

Međutim, kao i većina ostalih profesionalnih rješenja, i ovakvo rješenje je dosta skupo. Cijena NSX-a u Enterprise verziji kreće se u razini oko 7000$ po CPU jezgri ESXi poslužitelja, a cijena SRM-a u Enterprise verziji kreće se u razini oko 13000$ za 25 virtualnih poslužitelja. Cijene Standard verzija su niže, ali njima nedostaju mnoge bitne funkcionalnosti te je njihova učinkovitost kod oporavka od katastrofe slabija. Prema tome, za veći informacijski sustav od desetak ESXi poslužitelja i nekoliko stotina virtualnih poslužitelja cijena NSX-a i SRM-a s podrškom proizvođača bit će u milijunskim iznosima.

5. Alternativno rješenje (VMware Metro Storage Cluster)

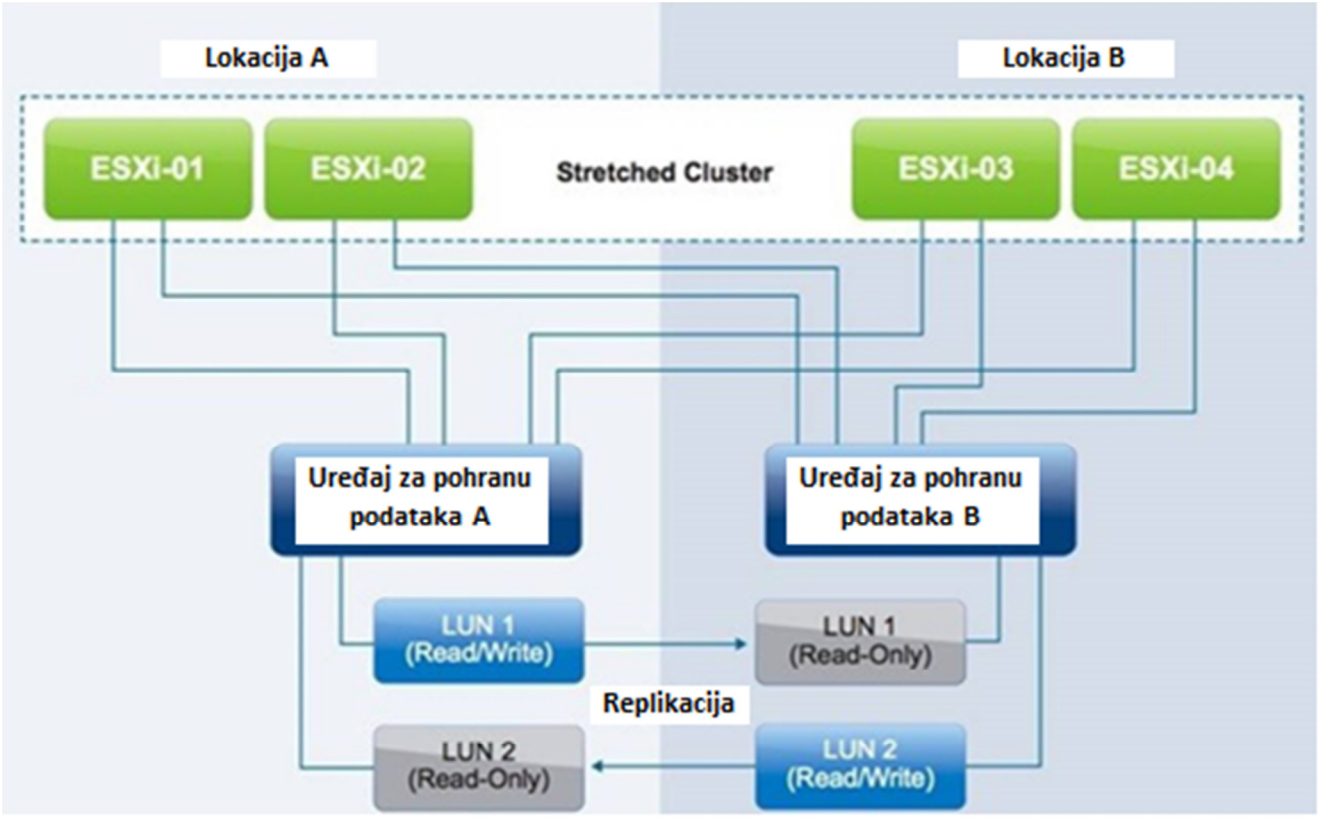
Velike tvrtke, organizacije ili državna tijela mogu imati vlastitu optičku infrastrukturu za povezivanje više podatkovnih centara u manjem geografskom području, najčešće u jednom gradu. U Hrvatskoj je to slučaj kod Ministarstva obrane koje u Zagrebu ima optičku vezu između sjedišta Ministarstva i dvije vojarne na različitim lokacijama u gradu. Izravna optička veza omogućava uporabu rješenja **VMware Metro Storage Cluster (vMSC)** koje je kao dodatna funkcionalnost uključena u standardnu VMware vSphere licencu te ne zahtjeva dodatne financijske izdatke. Ovo rješenje temelji se na VMware ESXi grupi (VMware clusteru) koji je rastegnut na dvije lokacije (engl. streched cluster). Njegovim korištenjem postiže se da su podatkovni centri na obje lokacije u potpunosti aktivni te je omogućena fleksibilnost i mobilnost radnog opterećenja između njih [**61**].

Temelj za korištenje ovog rješenja je optička veza koja omogućuje povezivost po podatkovnom (drugom) sloju OSI modela. Na taj način postiže se da je ista lokalna računalna mreža (LAN) rastegnuta na više lokacija. Zbog toga poslužitelji i uređaji za pohranu podataka mogu imati adrese unutar iste virtualne lokalne računalne mreže (engl. VLAN) što je temeljni preduvjet. ESXi poslužitelji na obje lokacije dio su istoga VMware vSphere clustera. vCenter Server koji upravlja svim ESXi poslužiteljima instaliran je na jednoj lokaciji. Svaka lokacija ima vlastiti uređaj za pohranu podataka koji moraju biti od istoga proizvođača. Upravljačka aplikacija od tog proizvođača (primjerice Dell, EMC, HP, IBM, NetApp) postavlja ta dva fizička uređaja u jedan dijeljeni razvučeni uređaj za pohranu podataka (engl. streched shared storage) na kojem je dostupan dijeljeni razvučeni logički diskovni prostor (engl. streched shared logical unit number, LUN) [**62**]. Organizacija vMSC rješenja na dvije lokacije prikazana je na slici 33.



Slika 33 – Organizacija VMware Metro Storage Cluster rješenja [62]

Opisana inačica implementacije vMSC rješenja prikazuje **uniformnu** konfiguraciju u kojoj svi ESXi poslužitelji imaju pristup na zajednički logički diskovni prostor razvučen na obje lokacije. U praksi to znači da poslužitelji na lokaciji A pristupaju na LUN1 koji je pohranjen



Slika 34 – Uniformna vMSC konfiguracija [61]

na uređaju na lokaciji A s pravima čitanja i pisanja (engl. read/write), a na kopiju LUN-a 2 čiji je original pohranjen na uređaju na lokaciji B samo s pravima čitanja (engl. read-only). Poslužitelji na lokaciji B pristupaju na LUN2 na uređaju na lokaciji B s pravima čitanja i pisanja, a na kopiju LUN-a 1 čiji je original pohranjen na uređaju na lokaciji A samo s pravima čitanja. Oba ta LUN-a se repliciraju s uređaja A na B i obrnuto [**61**]. Na taj način se oba LUN-a ponašaju kao dijeljeni razvučeni LUN-ovi kako je prikazano na slici 33. Veza ESXi poslužitelja i uređaja za pohranu podataka na dvije lokacije preciznije je prikazana na slici 34.

Prednosti korištenja vMSC rješenja u smislu oporavka od katastrofe su sljedeće [**62**]:

1. visoka dostupnost (engl. vSphere HA) virtualnih poslužitelja između dvije lokacije,
2. mogućnost migracije (engl. vSphere vMotion) virtualnih poslužitelja između dvije lokacije,
3. nastavak rada bez prekida u slučaju ispada uređaja za pohranu podataka na jednoj lokaciji,
4. nastavak rada bez prekida u slučaju ispada cijele jedne lokacije,
5. automatsko pokretanje failover procedura.

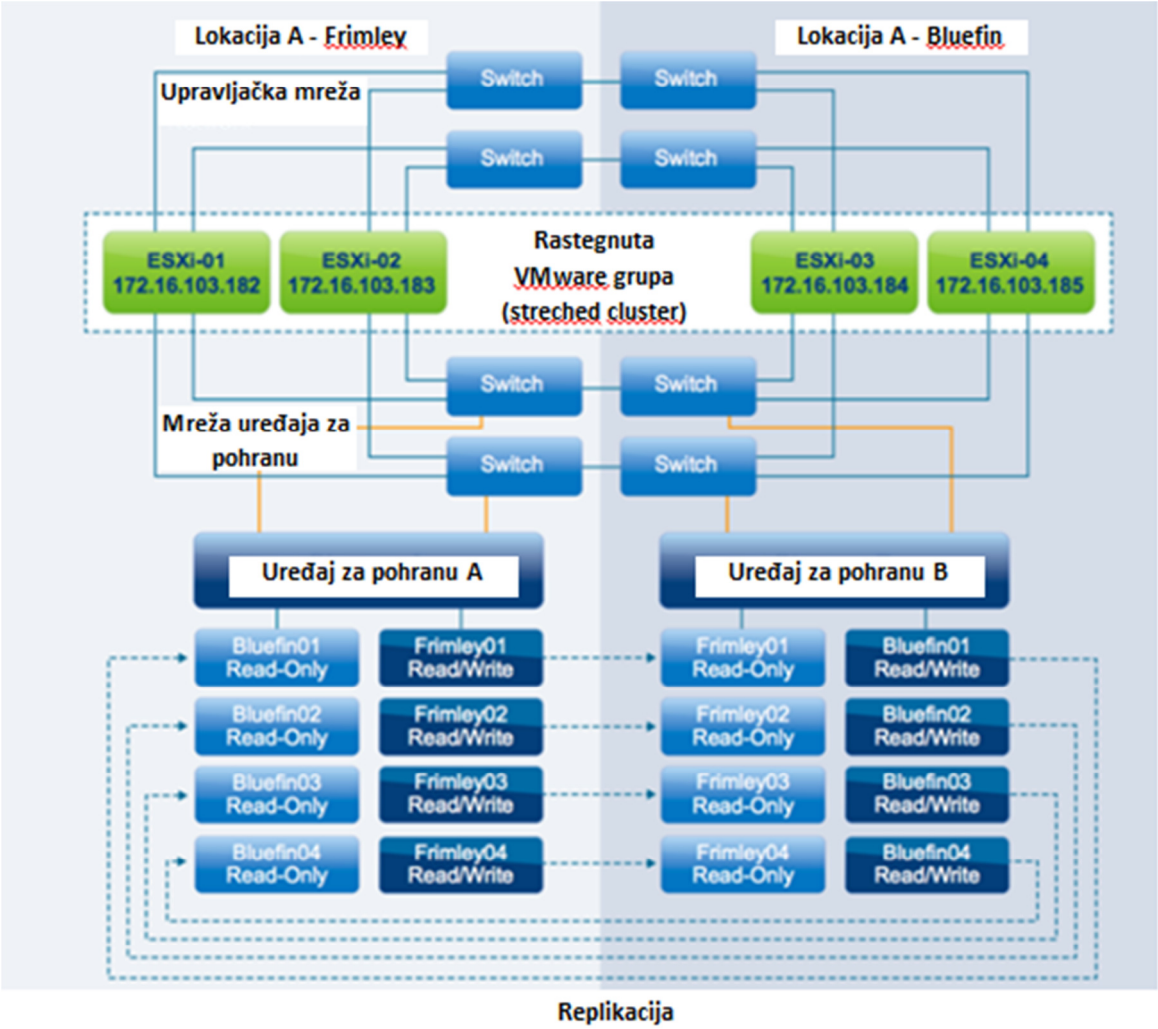
Drugim riječima, prilikom primjene vMSC rješenja oporavak od nedostupnosti poslužitelja, jednog od dva uređaja za pohranu podataka ili cijele lokacije omogućuju servisi vSphere HA i vMotion koji su uključeni u vSphere Standard ediciju te vSphere DRS koji je uključen u vSphere Enterprise plus ediciju. HA ili visoka dostupnost je servis koji se aktivira kad neki od ESXi poslužitelja postane nedostupan ili ima probleme u radu. HA automatski prebacuje virtualne poslužitelje s nedostupnog na drugi, dostupni i aktivni ESXi poslužitelj te ih tamo uključuje. DRS (engl. Distributed Resource Scheduler) osigurava uravnoteživanje opterećenja (engl. load balancing) unutar vSphere clustera. Taj servis raspoređuje virtualne poslužitelje na ESXi poslužitelje koji imaju dovoljno raspoloživih hardverskih resursa za njihovo pokretanje. U slučaju ako jedan ESXi poslužitelj postane preopterećen, DRS će automatski rasporediti virtualne poslužitelje s njega na druge ESXi poslužitelje koji su pod manjim opterećenjem [**63**]. vMotion omogućuje selidbu uključenog virtualnog poslužitelja s jednog na drugi ESXi poslužitelj. To je moguće zato što su svi diskovi, stanje memorije i aktivnih aplikacija te mrežnih postavki virtualnog poslužitelja pohranjeni na diskovnom prostoru koji je zajednički za sve ESXi poslužitelje. Virtualni poslužitelj migrira se u aktivnom stanju te nema nikakvog prekida njegove dostupnosti za korisnike [**64**].

5.1. Oporavak od katastrofe u slučaju nedostupnosti cijele lokacije

vMSC rješenje može se koristiti u različitim scenarijima oporavka – u slučaju nedostupnosti poslužitelja, LUN-a, cijelog uređaja za pohranu podataka do nedostupnosti cijele lokacije. U uobičajenom slučaju konfiguracije na dvije lokacije, svaka lokacija ima najmanje dva ESXi poslužitelja i jedan uređaj za pohranu podataka, a vCenter Server instaliran je na prvoj lokaciji. Lokacije su povezane izravnom optičkom vezom pomoću koje je na obje razvučena ista lokalna mreža (LAN). To znači da ESXi poslužitelji te uređaji za pohranu podataka imaju adrese iz istog adresnog raspona, a svaka lokacija ima svoju virtualnu izolacijsku adresu u istom rasponu. Primjer opisan u VMware-ovom dokumentu o preporučenim praksama za instalaciju vMSC-a prvu lokaciju naziva **Frimley**, a drugu **Bluefin** [**61**]. Na svakom uređaju za pohranu podataka instalirana su četiri LUN-a, a ukupno ih je osam. vMSC konfiguracija je uniformna što znači da svi ESXi poslužitelji imaju pristup na LUN-ove na oba uređaja za pohranu podataka. Na vCenter Serveru podešene su HA i DRS postavke kojima se za pojedine virtualne poslužitelje definiraju preferirani ESXi poslužitelji na kojima se ovi nalaze u uobičajenoj situaciji te pravila za selidbu s jednog ESXi poslužitelja na drugi u slučaju njegove nedostupnosti ili preopterećenja. Postavke za pojedinu lokaciju vMSC rješenja opisanog u VMware-ovom dokumentu prikazane su u tablici 1, a njegova shema na slici 35.

Lokacija	ESXi poslužitelj	Logički diskovni prostor (LUN)	Virtualna izolacijska adresa
Frimley	172.16.103.182	Frimley1	172.16.103.10
	172.16.103.183	Frimley2	
		Frimley3	
		Frimley4	
Bluefin	172.16.103.184	Bluefin1	172.16.103.11
	172.16.103.185	Bluefin2	
		Bluefin3	
		Bluefin4	

Tablica 1 - Primjer vMSC rješenja, postavke [61]



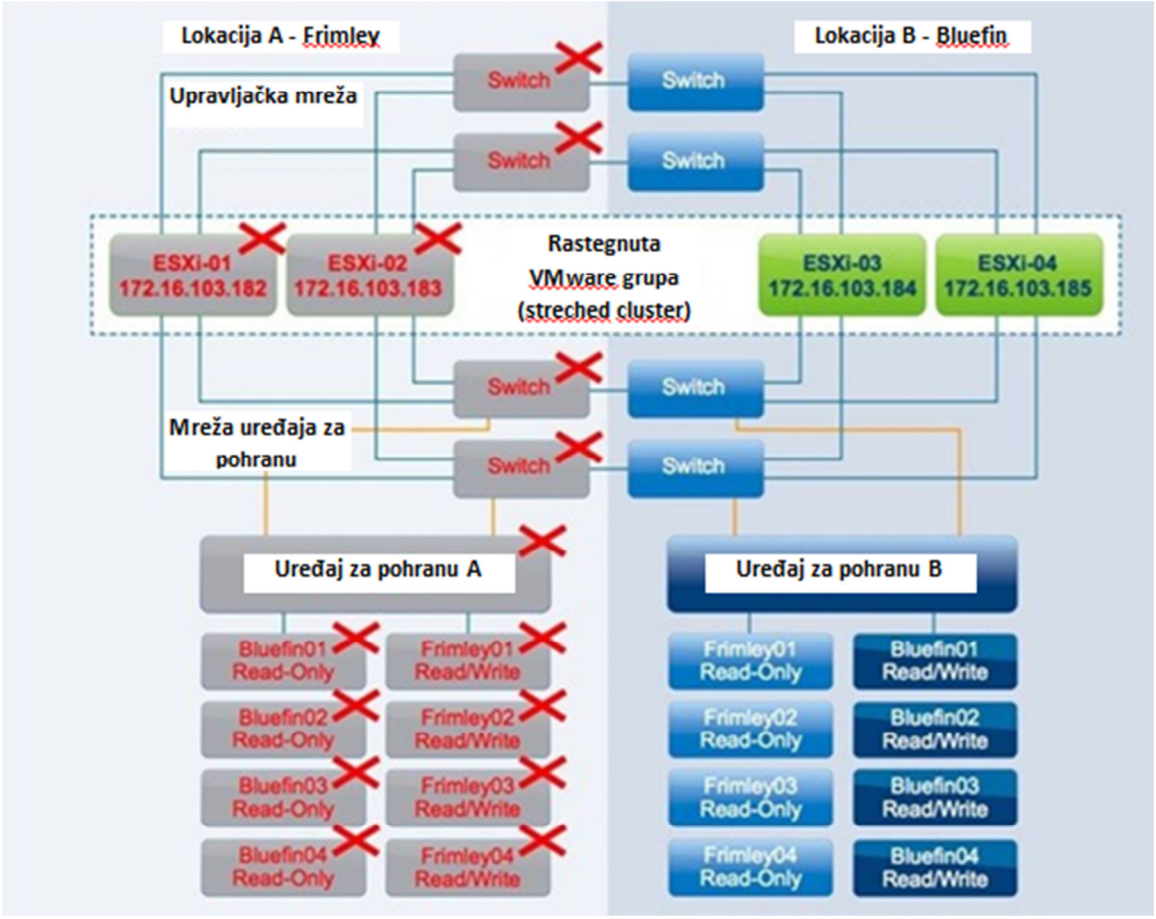
Slika 35 – Primjer vMSC rješenja, shema [61]

U slučaju katastrofe koja uzrokuje potpunu nedostupnost lokacije Frimley događa se sljedeće [**61**]:

1. vSphere HA servis na lokaciji Bluefin detektira da su poslužitelji na lokaciji Frimley postali nedostupni te preuzima primarnu ulogu,
2. uređaj za pohranu podataka B aktivira read-only kopije LUN-ova s lokacije Frimley čime oni prelaze u read/write stanje; ovu aktivnost provodi upravljački softver proizvođača uređaja za pohranu koji dolazi instaliran na njemu,
3. vSphere HA servis detektira virtualne poslužitelje koji se nalaze na Frimleyevim LUN-ovima,

4. vSphere HA servis uključuje virtualne poslužitelje koji se nalaze na Frimleyevim LUN-ovima.

Opisana situacija prikazana je na slici 36. U konačnici se svi virtualni poslužitelji aktiviraju na ESXi poslužiteljima na lokaciji Bluefin nakon čega korisnici opet imaju potpunu dostupnost svih servisa. Ako je vMSC konfiguriran ispravno, prekid rada do potpunog oporavka svih poslužitelja traje oko deset minuta.



Slika 36 – vMSC, nedostupnost cijele lokacije [61]

Nedostatci vMSC rješenja proizlaze iz toga što ono u osnovi nije zamišljeno kao alat za oporavak od katastrofe (disaster recovery), nego kao alat za izbjegavanje katastrofe (engl. disaster avoidance). Njegova uloga je smanjenje mogućnosti za nastanak katastrofe u slučaju nedostupnosti jednog od ESXi poslužitelja, LUN-a ili cijelog uređaja za pohranu podataka. U slučaju nedostupnosti cijele lokacije, vMSC će odraditi aktivaciju virtualnih poslužitelja na drugoj lokaciji, ali uz određenja ograničenja. Primjerice, vMSC ne omogućuje povratak neke povijesne točke oporavka (engl. recovery point) nego osposobljava nedostupne virtualne poslužitelje u njihovom posljednjem aktivnom stanju. Osim toga, postoji i tehničko

ograničenje uzrokovano mrežnom latencijom zbog čega lokacije ne mogu biti previše udaljene, maksimalno do 100 km. Specijalizirana rješenja za oporavak od katastrofe u pravilu omogućuju povratak prethodnih točki oporavka za pojedine poslužitelje i aplikacije instalirane na njima. Također se ne može sa sigurnošću znati hoće li se aplikacije koje će se izvršavati na virtualnim poslužiteljima oporavljenima na drugoj lokaciji kad virtualni poslužitelji na originalnoj lokaciji postanu nedostupni i dalje izvršavati na zadovoljavajući način. I na kraju, vMSC ne daje mogućnost testiranja oporavka od katastrofe. Njegova učinkovitost može se provjeriti jedino ako jedna od dvije lokacije stvarno postane nedostupna, a to se ne želi umjetno izazivati u svrhu testiranja [**62**].

6. Zaključak

Upravljanje kontinuitetom poslovanja je poslovna funkcija koja ima velik utjecaj na cjelokupno poslovanje organizacije, ali često nije dovoljno prepoznata. Razlog tome je što sve aktivnosti vezane uz nju iziskuju značajne organizacijske i ljudske napore te financijske izdatke čiji se rezultati ne vide izravno, primjerice, kroz analizu poslovnih učinaka na kraju godine. Organizacija koja ulaže u taj segment poslovanja izrađujući, implementirajući te testirajući planove upravljanja kontinuitetom poslovanja u stvari se nada da ih nikada neće morati primijeniti u praksi. Prema tome, troškovi rada u tom području poslovanja su opipljivi, a rezultati su često nevidljivi, osim kada se katastrofa stvarno dogodi.

Zbog važnosti koje u suvremenom poslovanju imaju informacijski sustavi, zaštita informacijskih resursa osobito je važan segment upravljanja kontinuitetom poslovanja. U principu, neprekidnost poslovanja praktički u svim slučajevima podrazumijeva i neprekidnost dostupnosti servisa odnosno aplikacija informacijskog sustava. Suvremene IT tehnologije nude mnoga rješenja za neprekidnost poslovanja odnosno oporavak od katastrofe za informacijske sustave, a koja se temelje na oblaku. Poduzeća i organizacije mogu se odlučiti za eksternalizaciju (engl. outsourcing) raznih IT segmenata, od hardverske infrastrukture preko aplikacija do sigurnosti i izrade pričuvnih kopija podataka. To ubrzava implementaciju IT usluga, daje sigurnost u smislu tehničke potpore, smanjuje troškove i olakšava predviđanje financijskih izdataka.

Međutim, postoje organizacije koje koriste specifičnu vrstu informacijskog sustava, a to je izolirani informacijski sustav. To su organizacije koje zbog sigurnosnih ili zakonskih aspekata svoga poslovanja moraju izolirati svoj informacijski sustav od drugih, nesigurnih informacijskih sustava poput Interneta. Najčešći razlog za to je taj što on sadrži klasificirane podatke ili je vezan uz posebno osjetljiv poslovni proces poput kontrole leta ili upravljanja postrojenja nuklearne elektrane. Takve organizacije ne koriste eksternalizaciju nego svoj informacijski sustav drže na vlastitoj lokaciji te na vlastitoj hardverskoj i softverskoj infrastrukturi. Zbog iznimne osjetljivosti informacijskog sustava koji koriste one moraju osigurati redundanciju lokacije i opreme kako bi izbjegle mogućnost jedne točke kvara kojom bi njihov sustav postao nedostupan ili izgubio podatke. Iz tog razloga moraju uspostaviti

dodatni podatkovni centar, idealno na drugom potresnom području na koji se mogu prebaciti IT servisi odnosno aplikacije s primarne lokacije u slučaju ispada odnosno katastrofe. Kako bi se omogućio nastavak rada informacijskog sustava na lokaciji pričuvnog podatkovnog centra u slučaju ispada primarne lokacije, između njih mora postojati kvalitetna mrežna veza, podatci se moraju učestalo replicirati s primarne na pričuvnu lokaciju te mora postojati softversko rješenje koje se brine za aktivaciju IT servisa na pričuvnoj lokaciji u slučaju katastrofe.

Kako bi izolirani informacijski sustav na kvalitetan način ispunjavao svoju ulogu, mora biti sagrađen na kvalitetnoj hardverskoj i softverskoj infrastrukturi. Tvrtka VMware predvodnik je za virtualizacijske tehnologije te je većina velikih informacijskih sustava u svijetu instalirana na okruženjima koja sadrže njihove ESXi fizičke poslužitelje, VMware virtualne poslužitelje te vCenter Server kao upravitelj. U tom slučaju se VMware NSX i SRM mogu jednostavno primijeniti kao rješenja za oporavak od katastrofe budući da su utemeljena na istoj tehnologiji. Jeftinija alternativa je korištenje VMware Metro Storage Cluster rješenja koje nije idealno budući da zahtijeva da organizacija ima vlastitu optičku vezu odnosno povezivost po podatkovnom (drugom) sloju OSI modela između lokacija te da lokacije zbog mrežne latencije ne mogu biti previše udaljene, maksimalno do 100 km.

Odgovornost za proces upravljanja kontinuitetom poslovanja leži na upravi organizacije, ali IT odjel često je taj koja mora osvijestiti tu problematiku upravi, osobito u segmentu važnosti neprekidne dostupnosti informacijskog sustava za cjelokupno poslovanje. Prema tome, kako bi se uopće razmatralo primjenu sustava za oporavak od katastrofe u IT području, prvo i najvažnije je da uprava organizacije osvijesti potrebu za procesom upravljanja kontinuitetom poslovanja jer u slučaju katastrofe za improvizaciju je prekasno.

7. Literatura

[1] Business Continuity Institute. (2010, Ožujak) The business case for BCM (full report). [Online]. https://www.thebci.org/resource/the-business-case-for-bcm--full-report-.html

[2] IBM. (2007, Veljača) "IBM System Storage Business Continuity Solutions Overview". [Online]. https://www.redbooks.ibm.com/redbooks/pdfs/sg246684.pdf

[3] Business Continuity Institute. (2018, Studeni) BCI Continuity and Resilience Report 2018. [Online]. https://www.thebci.org/resource/bci-continuity-and-resilience-report-2018.html

[4] Andrew Hiles, *"The Definitive Handbook of Business Continuity Management"*, 2nd ed. West Sussex PO19 8SQ, England: John Wiley & Sons Ltd, 2007.

[5] Michael E Whitman and Herbert J Mattord, *Principles of Information Security*, 6th ed. Boston, MA 02210, SAD: Cengage Learning, 2018.

[6] National Institute of Standards and Technology, U.S. Department of Commerce. (2010, Svibanj) "NIST Special Publication 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems". [Online]. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

[7] National Institute of Standards and Technology, U.S. Department of Commerce. (2012, Kolovoz) "NIST Special Publication 800-61 Rev. 2, Computer Security Incident Handling Guide". [Online]. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[8] Susan Snedaker, *"Business Continuity & Disaster Recovery for IT Professionals"*, 2nd ed. Waltham, MA 02451, SAD: Syngress, 2014.

[9] International Organization for Standardization, "ISO 31000, Risk management - Guidelines", Feb. 15, 2018.

[10] Hrvatska agencija za nadzor financijskih usluga. (2014, Listopad) "Smjernice za primjereno upravljanje rizicima informacijskih sustava subjekata nadzora". [Online]. https://www.hanfa.hr/getfile/41744/7-Smjernice%20za%20primjereno%20upravljanje%20rizicima%20IS%20subjekata%20nadzora%20Agencije.pdf

[11] International Organization for Standardization, "ISO/IEC 27002, Information technology—Security techniques — Code of practice for information security controls", Oct. 01, 2013.

[12] Michael Morfoot. (2009, Rujan) Department of Computer and Mathematical Sciences. [Online]. http://cs.lewisu.edu/mathcs/msis/projects/msis595_MichaelMorfoot.pdf

[13] Silvana Tomić Rotim and Višnja Komnenić. (2017, Svibanj) "Dani kriznog upravljanja - Kako pripremiti sveobuhvatan plan kontinuiteta poslovanja?" [Online]. http://dku.hr/wp-content/uploads/2017/05/Zbornik_Radova_2017.pdf

[14] Jon Granados. SADOS Web site. [Online]. https://sados.com/blog/types-of-disaster-recovery-plans/

[15] Barracuda Networks, Inc. "What You Must Know about 7 Tiers of Disaster Recovery". [Online]. https://www.dashtech.org/what-you-must-know-about-7-tiers-of-disaster-recovery/

[16] Jessie Reed. (2019, Siječanj) "An Overview of Disaster Recovery Sites". [Online]. https://www.nakivo.com/blog/overview-disaster-recovery-sites/

[17] Wikipedia. (2020, Prosinac) Failover. [Online]. https://en.wikipedia.org/wiki/Failover

[18] Microsoft. (2020, Srpanj) Switchovers and Failovers. [Online]. https://docs.microsoft.com/en-us/exchange/switchovers-and-failovers-exchange-2013-help?redirectedfrom=MSDN

[19] Wikipedia. (2019, Kolovoz) Switchover. [Online]. https://en.wikipedia.org/wiki/Switchover

[20] Techopedia. (2021, Siječanj) Fallback. [Online]. https://www.techopedia.com/definition/27071/failback

[21] Software Testing Help. (2021, Veljača) "Top 5 BEST Disaster Recovery Services & Software Companies 2021". [Online]. https://www.softwaretestinghelp.com/best-disaster-recovery-services-and-software-tools/

[22] Markets and Markets. (2020, Studeni) "DRaaS Market by Service Type (Backup and Restore, Real-Time Replication, and Data Protection), Deployment Model (Public Cloud and Private Cloud), Organization Size, Vertical, and Region - Global Forecast to 2025". [Online]. https://www.marketsandmarkets.com/Market-Reports/recovery-as-a-service-market-962.html

[23] IBM. (2020, Listopad) "IBM Backup as a ServiceDynamic cloud-based data protection solutions for optimal information resiliency". [Online]. https://www.ibm.com/downloads/cas/B9ER7D3P

[24] VEEAM. (2020, Listopad) "Veeam Cloud Connect Replication". [Online]. https://helpcenter.veeam.com/docs/backup/cloud/cloud_replication.html?ver=110

[25] Wikipedia. (2021, Svibanj) Hypervisor. [Online]. https://en.wikipedia.org/wiki/Hypervisor

[26] Microsoft. (2020, Ožujak) "SMB disaster recovery with Azure Site Recovery". [Online]. https://docs.microsoft.com/en-us/azure/architecture/solution-ideas/articles/disaster-recovery-smb-azure-site-recovery

[27] Protiviti Inc. (2020, Srpanj) "Top Business Continuity Management and Planning Questions". [Online]. https://www.protiviti.com/sites/default/files/guide-to-business-continuity-management-top_15_faqs_july_2020_global.pdf

[28] Business Continuity Management Institute. (2018, Siječanj) "What exactly is BCM?" [Online]. https://blog.bcm-institute.org/bcm/what-exactly-is-business-continuity-management

[29] CARNet. (2010, Srpanj) "Upravljanje kontinuitetom poslovnih procesa“, NCERT-PUBDOC-2010-07-307. [Online]. https://www.cert.hr/upravljanje-kontinuitetom-poslovnih-procesa/

[30] Ponemon institute. (2016, Siječanj) “2016 Cost of Data Center Outages”. [Online]. https://www.ponemon.org/blog/2016-cost-of-data-center-outages

[31] Disasterrecovery.org. (2020, Prosinac) IT Business Continuity. [Online]. https://www.disasterrecovery.org/it-business-continuity/

[32] Hwaiyu Geng, *Data Center Handbook*. Hoboken, New Jersey, SAD: John Wiley & Sons, Inc, 2015.

[33] Networkworld. (2020, Veljača) For secure data backup, here’s how to do the 3-2-1 rule right. [Online]. https://www.networkworld.com/article/3527303/for-secure-data-backup-here-s-how-to-do-the-3-2-1-rule-right.html

[34] Wikipedia. (2021, Veljača) Data center. [Online]. https://en.wikipedia.org/wiki/Data_center

[35] Wikipedia. (2021, Veljača) TIA-942. [Online]. https://en.wikipedia.org/wiki/TIA-942

[36] Wikipedia. (2021, Ožujak) Availability. [Online]. https://en.wikipedia.org/wiki/Availability

[37] Uptime Institute. (2020, Srpanj) Uptime Institute global data center survey 2020. [Online]. https://drift-lp-66680075.drift.click/UptimeInstituteGlobalDataCenterSurvey2020

[38] VMware. (2021, Siječanj) Software-Defined Datacenter – In Depth. [Online]. https://www.vmware.com/solutions/software-defined-datacenter/in-depth.html#compute

[39] Cynthia Harvey. (2017, Srpanj) What is an SDDC? Benefits & Challenges. [Online]. https://www.datamation.com/data-center/what-is-sddc/

[40] VMware. (2015, Srpanj) VMware Software-Defined Data Center - TECHNICAL WHITE PAPER. [Online]. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/technical-whitepaper-sddc-capabilities-itoutcomes-white-paper.pdf

[41] Thales. (2021, Siječanj) Network Encryption. [Online]. https://www.thalesgroup.com/en/network-encryption

[42] Zavod za sigurnost informacijskih sustava. (2018, Svibanj) Registar odobrenih

kriptografskih uređaja. [Online]. https://www.zsis.hr/default.aspx?id=55

[43] Ahmed Humair. (2017, Siječanj) VMware NSX and SRM: Disaster Recovery Overview and Demo. [Online]. https://blogs.vmware.com/networkvirtualization/2017/01/vmware-nsx-srm-disaster-recovery-overview-demo.html/

[44] VMware. (2017, Travanj) VMware NSX for Disaster Recovery. [Online]. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-nsx-for-disaster-recovery-guide.pdf

[45] Ahmed Humair. (2018, Kolovoz) VMware NSX Multi-site Solutions and Cross-vCenter NSX Design Day 1. [Online]. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-multi-site-solutions-cross-vcenter-nsx-design-guide.pdf

[46] Icy Science. (2021, Siječanj) Što je hipervizor? - definicija iz tehopedije. [Online]. https://hr.icyscience.com/hypervisor

[47] VMware. (2019, Svibanj) Cluster Types. [Online]. https://docs.vmware.com/en/VMware-Validated-Design/5.0/com.vmware.vvd.sddc-design.doc/GUID-355BFCFA-3F80-4AB8-BC7A-115AAF40CA55.html

[48] VMware. (2016, Travanj) Disaster Recovery with NSX and SRM. [Online]. https://communities.vmware.com/t5/VMware-NSX-Documents/Disaster-Recovery-with-NSX-and-SRM/ta-p/2789808

[49] Abhilash GB, *Disaster Recovery Using VMware vSphere Replication and vCenter Site Recovery Manager*. Birmingham, UK: Packt Publishing Ltd, 2014.

[50] IT Central Station. (2021, Ožujak) VMware NSX Reviews. [Online]. https://www.itcentralstation.com/products/vmware-nsx-reviews

[51] IT Central Station. (2021, Ožujak) VMware SRM Reviews. [Online]. https://www.itcentralstation.com/products/vmware-srm-reviews

[52] Controlup. (2018, Studeni) Hypervisor Market Share – ControlUp Perspective. [Online].

https://www.controlup.com/resources/blog/entry/hypervisor-market-share-controlup-perspective/

[53] DNSstuff. (2020, Travanj) Best Server Virtualization Software. [Online]. https://www.dnsstuff.com/server-virtualization-software

[54] Gartner Peer Insights. (2021, Svibanj) VMware NSX Data Center Alternatives. [Online]. https://www.gartner.com/reviews/market/data-center-and-cloud-networking/vendor/vmware/product/vmware-nsx/alternatives

[55] G2. (2021, Ožujak) Compare Cisco ACI and NSX. [Online]. https://www.g2.com/compare/cisco-aci-vs-nsx

[56] VMware. (2018, Srpanj) SDN - Cisco ACI Vs NSX. [Online]. https://communities.vmware.com/t5/VMware-NSX-Discussions/SDN-Cisco-ACI-Vs-NSX/td-p/1426645

[57] IT Central Station. (2021, Ožujak) VMware NSX Room for Improvement. [Online]. https://www.itcentralstation.com/products/vmware-nsx-room-for-improvement?tid=pdf_cat_2035

[58] Fujitsu. (2010, Studeni) Disaster recovery with Eternus DX – the data safe – and VMware SRM. [Online]. https://www.fujitsu.com/global/Images/dx-vmware-srm.pdf

[59] IT Central Station. (2021, Ožujak) VMware SRM Room for Improvement. [Online]. https://www.itcentralstation.com/products/vmware-srm-room-for-improvement

[60] VMware. (2020, Svibanj) The Total Economic Impact™ of VMware NSX & SRM. [Online]. https://www.vmware.com/content/dam/learn/en/amer/fy21/pdf/558734_21Q2_WW_ALL_WebForm_VCN_DCN_NSXTrailBlz_EN_REG_20220608.pdf

[61] VMware. (2020, Kolovoz) VMware vSphere Metro Storage Cluster Recommended Practices. [Online]. https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-recommended-practices#section1

[62] David Pasek. (2018, Prosinac) VCDX #200 Blog of one VMware Infrastructure Designer. [Online]. https://www.vcdx200.com/2018/12/vmware-metro-storage-cluster-is-it-dr.html

[63] Vembu. (2019, Rujan) VMware HA and DRS Explained. [Online]. https://www.vembu.com/blog/ha-vs-drs-in-vmware-vsphere/

[64] Niels Hagoort. (2019, Srpanj) VMware vSphere Blog. [Online]. https://blogs.vmware.com/vsphere/2019/07/the-vmotion-process-under-the-hood.html

[65] UMEA University. (2014, Travanj) Data Center Construction and Management. [Online]. http://www8.cs.umu.se/kurser/5DV131/VT14/handouts/L6_dcs.pdf

[66] NETARI. (2017, Siječanj) "What to Look for in a Data Center. Understanding Tier Levels & Industry Standards." [Online]. https://www.netari.com/post/2014/02/04/what-to-look-for-in-a-data-center-understanding-tier-levels-industry-standards

[67] Energy Star. (2012, Rujan) Server Virtualization. [Online]. https://www.energystar.gov/products/low_carbon_it_campaign/12_ways_save_energy_data_center/server_virtualization

[68] Ahmed Humair. (2017, Veljača) NSX-V 6.3: Cross-VC NSX Security Enhancements. [Online]. https://blogs.vmware.com/networkvirtualization/2017/02/nsx-6-3-cross-vc-nsx-security-enhancements.html/

[69] Consolidated Technologies, inc. (2018, Lipanj) Outsourced IT Services. [Online]. https://consoltech.com/blog/benefits-and-risks-of-managed-it-services/

[70] KeepItSafe. (2019, Studeni) Disaster Recovery for vSphere: How DRaaS Outperforms Object Storage. [Online]. https://www.keepitsafe.com/blog/post/disaster-recovery-for-vsphere-how-draas-outperforms-object-storage/

[71] TechTarget. (2014, Ožujak) VMware vSphere Metro Storage Cluster (VMware vMSC). [Online]. https://searchservervirtualization.techtarget.com/definition/VMware-vSphere-Metro-Storage-Cluster-VMware-vMSC

Sažetak

Naslov: Upravljanje kontinuitetom poslovanja u kontekstu izoliranog informacijskog sustava.

Rad obrađuje područje planiranja za nepredviđene okolnosti. Definira osnovne pojmove, opisuje analizu utjecaja na poslovanje, upravljanje rizicima, odgovor na incident, oporavak od katastrofe te upravljanje kontinuitetom poslovanja. Pri tome se podrazumijeva da je većina informacijskih sustava povezana s Internetom ili drugim informacijskim sustavima. Međutim, pojedine organizacije zbog sigurnosnih ili zakonskih aspekata svoga poslovanja moraju izolirati svoj informacijski sustav od drugih, manje sigurnih informacijskih sustava. Takve organizacije svoj informacijski sustav drže na vlastitoj lokaciji u vlastitom podatkovnom centru te na vlastitoj hardverskoj i softverskoj infrastrukturi, čemu je u radu posvećena posebna pažnja. Razmotreni su preduvjeti i mogućnosti oporavka izoliranog informacijskog sustava te je predloženo rješenje koje osigurava redundanciju lokacije i opreme na pričuvnoj lokaciji u pričuvnom podatkovnom centru, podržano odgovarajućim tehnologijama kojima se informatički resursi (mreža, poslužitelji i aplikacije) repliciraju s primarne na pričuvnu lokaciju u svrhu oporavka od katastrofe. Procijenjeno je i alternativno, jeftinije, rješenje koje pretpostavlja da organizacija ima vlastiti mrežni spojni put (primjerice, optički kabel) između primarne i pričuvne lokacije.

Ključne riječi: planiranje za nepredviđene okolnosti, upravljanje kontinuitetom poslovanja, oporavak od katastrofe, izolirani informacijski sustav, podatkovni centar, redundancija, VMware NSX, VMware SRM, VMware Metro Storage Cluster

Abstract

Title: Business continuity management in the context of an isolated information system.

The thesis deals with the topics of contingency planning. It defines the basic concepts, describes the business impact analysis, risk management, incident response, disaster recovery and business continuity management. It is implied that most of the information systems are connected to Internet or other information systems. However, due to security or legal aspects of their business, certain organizations must isolate their information system from other, less secure information systems. Such organizations keep their information system at their own location in their own data center and on their own hardware and software infrastructure, to which special attention is paid in the thesis. The preconditions and possibilities for the recovery of an isolated information system are considered and a solution is proposed that ensures the redundancy of the location and equipment at the backup location in the backup data center and which is supported by appropriate technologies by which IT resources (network, servers and applications) are replicated from the primary to the backup location for disaster recovery. An alternative, cheaper, solution that assumes that the organization has its own network connection path (e.g., an optical cable) between the primary and backup locations has also been evaluated.

Keywords: contingency planning, business continuity management, disaster recovery, isolated information system, data center, redundancy, VMware NSX, VMware SRM, VMware Metro Storage Cluster

Životopis

Ivan Račić rođen je 1979. godine u Zagrebu. Diplomirao je 2002. godine na Ekonomskom fakultetu u Zagrebu, smjer Poslovna informatika. Nakon kraćeg rada u informatičkom odjelu u privatnom poduzeću, 2003. godine zaposlio se u Ministarstvu obrane gdje radi i danas. Karijeru je započeo kao pripravnik u informatici. Dvije godine kasnije završio je časničku školu te karijeru nastavio kao časnik oružanih snaga. Završio je razne edukacije iz informatičkog područja uključujući Cisco CCNA akademiju, IBM Lotus Domino Server, VMware vSphere Install, Configure & Manage. Danas radi kao specijalist za mreže i Windows poslužitelje. Ima Cisco CCNP i IBM Lotus Domino industrijski certifikat.

Biography

Ivan Račić was born in 1979. in Zagreb. In 2002. he graduated on Faculty of Economics and Business in Zagreb on Business Informatics study program. After short time in IT department of a private company, in 2003. he gained employment in Ministry of Defense where he works today. He began his career as a trainee in IT department. Two years later he finished the officer's course and continued his career as an officer of Armed Forces. He finished different IT educations including Cisco CCNA Academy, IBM Lotus Domino Server, VMware vSphere Install, Configure & Manage. Today he works as networking and Windows server specialist. He holds Cisco CCNP and IBM Lotus Domino industrial certificates.