CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Upravljanje kontinuitetom poslovnih procesa

NCERT-PUBDOC-2010-07-307

Nacionalni CERT

u suradnji s

LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem Nacionalni CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom Nacionalnog CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

Nacionalni CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Istraživanja provedena na institutu za kontinuitet poslovanja, Bussines Continuity Institute (BCI) pokazala su da će u prosjeku 20% svih organizacija iskusiti neki oblik neplaniranog događaja barem jednom u svakih pet godina. Možda to neće biti događaj katastrofalnih razmjera kojima se pune naslovnice novina, no to ne umanjuje potrebu za razmišljanjem o izglednijim događajima poput nestanka struje ili kvara IT opreme nužne za poslovanje. Gotovo 90% kriza nije dramatično poput onih medijski eksponiranih, ali upravo one imaju potencijal oštetiti najveće vrijednosti kompanije: njezino ime i reputaciju. Popravak kritičnog poslužitelja nije dovoljan za nastavak poslovanja ako zaposlenici nemaju gdje obavljati svoj posao. Dugotrajniji gubitak struje, nedostupnost telefonske i/ili Internet veze, krađe i slični incidenti nisu više problem isključivo IT odjela nego cijele organizacije.

Izrada plana kontinuiteta poslovanja osnovni je korak koji neka organizacija mora poduzeti na putu do dobro definiranog i upravljivog procesa upravljanja kontinuitetom poslovanja. S obzirom da je izrada plana ponekad složenija i od samih mjera koje se njime predviđaju, mnoge organizacije izbjegavaju njegovu izradu. Izrada plana kontinuiteta poslovanja se upravi organizacije obično prikaže kao investicija vrijedna nekoliko stotina tisuća ili milijuna eura. Problemi nastanu radi činjenice da će ta investicija u pravilu biti isplativa možda jednom u dvadeset godina.

Kao primjer se može uzeti sljedeći scenarij koji je za razliku od kakvog razornog potresa gotovo pa svakodnevica u raznoraznim organizacijama. Dakle, scenarij je sljedeći :

„…Predsjednik uprave jednog je poslijepodneva primijetio da slanje i primanje jednostavne elektroničke pošte traje neuobičajeno dugo i da se gubi veza s poslužiteljem elektroničke pošte. Pokušao je nazvati informatičkog direktora, ali je na ekranu njegovog IP telefona pisalo da nema mreže. Mobilnim telefonom uspio je dobiti informatičkoga direktora koji mu je objasnio da nema razloga za brigu jer će uskoro ukloniti problem. Predsjednik uprave tražio je da problem riješe što prije jer mu je otežavao rad. Informatički direktor nazvao je voditelja svog IT odjela i pitao za fazu rješavanja problema. Voditelj mu je odgovorio da intenzivno rade na tome, ali da još nisu pronašli uzrok . Usput mu je objasnio da se isti problem ponavlja posljednjih nekoliko dana, i da to tako kratko traje i zatim nestane samo od sebe. Nažalost, ovaj put se stanje nije vratilo u normalu. Uskoro su počeli pozivi mobitelom zaposlenika iz središnjice i poslovnica banke s pritužbama da telefoni ne rade, poslovna aplikacija ne funkcionira i da se na šalterima stvaraju redovi nezadovoljnih korisnika …“

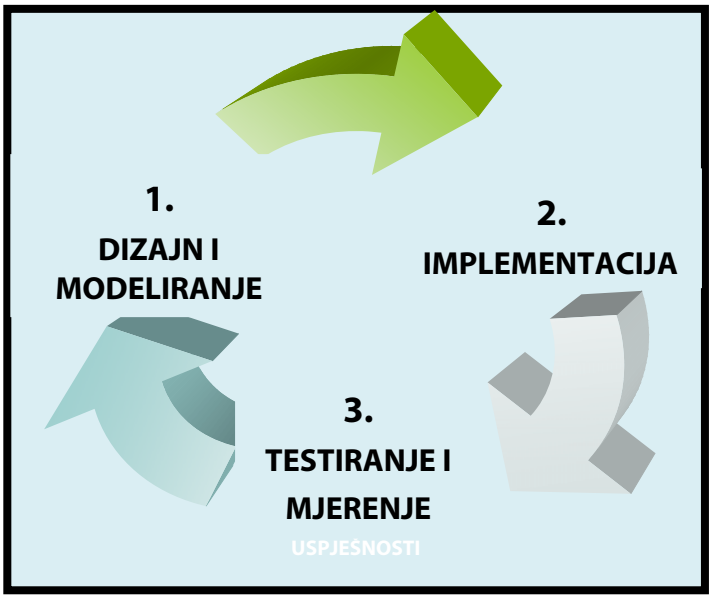
Problemi navedeni u ovom scenariju gotovo su svakodnevica velikih organizacija. Odgovor i rješenje pronalazi se u upravljanju kontinuitetom poslovnih procesa. U ovom dokumentu opisan je pojam upravljanja kontinuitetom poslovnih procesa, razrađene su strategije koje se primjenjuju u izradi plana kontinuiteta poslovanja te napravljene analize rizika i ponuđena potencijalna rješenja.

2. Poslovni procesi

Uspješne poslovne subjekte danas karakterizira kvaliteta, cijena, predanost kupcu te brzina reakcije i prilagodbe promjenama. Svaka organizacija mora znati što želi postići svojim poslovnim procesima. Poslovni sustavi s dobro ustrojenim poslovnim procesima ubrzavaju rad tvrtke kojoj pripadaju, povećavaju unutarnji red, smanjuju troškove te povećavaju kvalitetu proizvoda. Poslovno okruženje se neprekidno mijenja, brzina i količina promjena dramatično se povećava, konkurenti dolaze i nestaju, nestabilnost tržišta i globalizacija iz temelja mijenjaju način poslovanja. Neprekidno unaprjeđivanje poslovnih procesa jedan je od ključnih faktora uspjeha.

Iako je sam pojam poslovnog procesa prilično dugo prisutan, disciplina koja se bavi upravljanjem poslovnim procesima počela se razvijati tek posljednjih dvadesetak godina. Posljedica je to razvitka računala i softvera, povećanja njihovih mogućnosti i brzine rada.

Upravljanje poslovnim procesima ima nekoliko osnovnih aktivnosti. To su dizajn i modeliranje poslovnog procesa, izvođenje procesa te mjerenje njegove uspješnosti. U fazi dizajna, poslovni proces se opisuje, dokumentira te se utvrđuje važnost i značaj određenih parametara u tom procesu. Također, u ovoj fazi se može identificirati određeni postotak neefikasnih, nepotrebnih i/ili suvišnih procesa ili njihovih dijelova. Jednom opisani poslovni proces može poslužiti npr. za obuku novih djelatnika ili kao dio dokumentacije za dobivanje nekog industrijskog certifikata. U drugoj fazi proces se počinje izvoditi na način koji je opisan modeliranjem. Tada se sudionicima u procesu omogućuje da budu produktivniji jer u određenom trenutku znaju koji koraci su potrebni, koje su ulazne vrijednosti parametara i koji su očekivani rezultati za bilo koji korak u procesu. Jedini način da se zna je li poslovni proces dobar ili nije, jest da ga se prati i mjeri. Time se dolazi do treće faze koja se naziva faza praćenja ili nadzora. Što se mjeri, ovisi o procesu, grani djelatnosti, te cilju koji se želi ostvariti. Čak i ako nije poznato koji su ključni pokazatelji uspješnosti, samo mjerenje će kroz vrijeme pokazati napredak ili nazadovanje.



Slika 1. Dijagram upravljanja poslovnim procesima

Ono što upravljanju poslovnim procesima daje smisao jest neprekidno poboljšavanje poslovnog procesa na temelju mjerenja rezultata uspješnosti tog procesa.

Podaci o rezultatima uspješnosti, podaci o opisu poslovnih procesa, dokumentaciji itd. su danas najčešće pohranjeni u digitalnom obliku te je njihova sigurnost ugrožena sve većim brojem sigurnosnih prijetnji koje haraju Internetom. Pojam mrežne sigurnosti je danas neizbježan u poslovanju neke organizacije.

2.1. Informacijska sigurnost

Razvijene države (npr. SAD, Japan i UK) postavile su barem minimalne, a najčešće i odgovarajuće sigurnosne pravne standarde i kriterije informacijske sigurnosti. Nacionalnom politikom informacijske sigurnosti postavljaju opći okvir kojeg ostvaruju odgovarajućim zakonima kao što su:

- zakon o sigurnosnim službama,
- zakon o zaštiti tajnosti podataka,
- zakon o zaštiti osobnih podataka,
- zakon o pravu pristupa informacijama i
- kazneno zakonodavstvo

U poslovnim sustavima pravni okvir ovog područja čine i statut, sigurnosna politika tvrtke, pravilnici, sigurnosne procedure itd. Uzme li se u obzir činjenica da je informacijsko komunikacijska tehnologija infrastruktura svakog poslovanja, tada su brojne sigurnosne prijetnje (virusi, trojanski konji i dr.) prisutne na globalnoj Internet mreži izvor zahtjeva za odgovarajućom informacijskom sigurnosti. Brzi razvoj primjene informacijsko komunikacijske tehnologije uzrokuje sve veće mogućnosti napada na informacijske sustave i zlouporabu informacija, o čemu govore brojna upozorenja iz svijeta. O ovom aspektu postoje brojni i uglavnom dostupni izvori (FBI CSI, SANS Institute i dr.). Istraživanja navedenih institucija prikazuju da je godišnji porast broja napada na informacije kroz informatičke sustave negdje oko 90% i da broj novootkrivenih oblika ranjivosti informacijskih sustava raste eksponencijalno. Rastuće su i opasnosti od zatajenja informacijskih sustava, odnosno velikih šteta koje nastaju uslijed zastoja rada informacijskih sustava.

2.2. Kontinuitet poslovnih procesa

Osnovna ideja kontinuiteta poslovanja zapravo je zaštititi informacije u slučaju neke veće i neočekivane nezgode (dakle, osigurati dostupnost informacija). Nažalost, nezgode koje mogu biti kobne za poslovanje su sve više prisutne. Tu se ne misli samo na terorističke napade, nego i na potrese, požare, poplave, kvarove sklopovlja te programske podrške i sl. Upravljanje kontinuitetom poslovanja predviđa pisanje planova koji određuju na koji način je potrebno postupiti u izvanrednim situacijama (priprema rezervne lokacije, određivanje vremena oporavka, priprema komunikacije u slučaju krize i sl.). Krajem 2006. godine, objavljene su norme BS 25999-1 i BS 25999-2 koje detaljnije opisuju upravljanje kontinuitetom poslovanja.

Prema tim normama, plan kontinuiteta poslovanja mora se sastojati od :

1. **plana odaziva na incident**

Plan odaziva na incident obično je jedinstven plan koji se odnosi na cijelu organizaciju i opisuje radnje koje se moraju poduzeti odmah nakon pojave havarije – smanjenje posljedica incidenta, komunikacija sa službama za hitne slučajeve, evakuacija zgrade, okupljanje na zbornim mjestima, organizacija transporta na rezervnu lokaciju i sl.

2. **plana oporavka**

Plan oporavka se obično piše zasebno za svaku kritičnu aktivnost i mora obuhvaćati sljedeće korake:

- Vrijeme i način na koji se komunicira s raznim zainteresiranim stranama (zaposlenicima i njihovim obiteljima, dioničarima, klijentima, partnerima, državnim službama, javnim medijima i dr.),
- Princip sastavljanja tima,
- Provođenje oporavka infrastrukture,
- Provjera funkcionalnosti aplikacija i kontrole pristupa,
- Provjerava podataka koji nedostaju i utvrđivanje svega što je oštećeno u havariji,
- Oporavak podataka i uspostava normalnih aktivnosti.

O ovim normama više riječi će biti u sljedećim poglavljima.

2.3. Veza između kontinuiteta poslovnih procesa i informacijske sigurnosti

Na prvi pogled reklo bi se da kontinuitet poslovanja i informacijska sigurnost nemaju puno veze. No, iz dubljeg promatranja njihove povezanosti proizlazi zaključak da postoje poveznice, i to velike. Naime, informacijska sigurnost se brine o povjerljivosti, integritetu i dostupnosti (raspoloživosti) informacija u nekoj organizaciji, dok se kontinuitet poslovanja u prvom redu brine da su informacije dostupne onima koji ih trebaju. Suština kontinuiteta poslovanja jest da osigurava kontinuitet ključnih poslovnih procesa u nekoj organizaciji. Kako se svaki poslovni proces bazira na protoku informacija, tako je fokus kontinuiteta poslovanja na dostupnosti, odnosno očuvanju i oporavku vitalnih poslovnih informacija. Sličnosti postoje i u nekim provedbenim dokumentima. Na primjer, svaka metodologija za kontinuitet poslovanja propisuje potrebu procjene rizika, koja se provodi na isti način kao i procjena rizika za informacijsku sigurnost. Dakle, dio dokumentacije će biti zajednički i za kontinuitet poslovanja i informacijsku sigurnost.

S organizacijske strane isto tako postoje poveznice. Naime, vrlo često se funkcijska jedinica zadužena za brigu o kontinuitetu poslovanja nalazi baš unutar organizacijske jedinice koja je nadležna za informacijsku sigurnost.

3. Strategija i planiranje kontinuiteta poslovnih procesa

Strategija kontinuiteta poslovanja donosi niz stavki, koje u slučaju nezgode služe za uspostavu funkcionalnosti poslovanja. Bitne stavke strategije kontinuiteta poslovanja su.:

- Ciljano vrijeme oporavka za pojedine poslovno kritične funkcije (eng. RTO - *Recovery Time Objective*).
- Minimalne obveze koje se moraju izvoditi tijekom nezgode – u kritičnim situacijama vjerojatno neće biti moguće izvoditi pun opseg redovnih aktivnosti, pa treba odlučiti koje su nužne, a bez kojih se može (i koliku štetu one predstavljaju).
- Pronaći rezervnu lokaciju na kojoj će se ponovo uspostaviti svi poslovno kritični procesi, uključujući i IT infrastrukturu, obradu podataka i sl.
- Odrediti resurse koji će biti potrebni na rezervnoj lokaciji – ne samo računalne resurse, već i ljudske resurse, računalne servise te dokumente u papirnatom obliku i ostalu opremu.
- Članovi kriznog menadžmenta te zaduženja u situacijama nezgode.
- Ciljana točka oporavka za podatke, odnosno koliko unatrag će biti moguće rekonstruirati podatke ukoliko podaci budu uništeni u nezgodi. Ovaj zahtjev izravno određuje strategiju učestalosti izrade pričuvne pohrane podataka.
- Jedinstvene i kritične točke koje mogu prouzročiti prekid u radu. U preventivnim aktivnostima se treba fokusirati na to da se osigura bolja zaštita upravo tih resursa.
- Izvor i način nabave sve potrebne opreme u slučaju nezgode (ICT oprema, namještaj, vozila, strojevi, itd.).

3.1. Planiranje kontinuiteta poslovnih procesa

Planiranje kontinuiteta poslovanja je interdisciplinarna aktivnost, a obuhvaća metodologiju koja se koristi kako bi se stvorio praktičan plan oporavka. Plan koji opisuje način na koji će se organizacija oporaviti i vratiti u prijašnje stanje nakon djelomičnog ili potpunog prekida kritičnih poslovnih funkcija. Poseban naglasak nalazi se na realizaciji plana unutar unaprijed određenog vremena nakon nastupa prekida ili katastrofe.

Plan koji je rezultat te aktivnosti naziva se **planom kontinuiteta poslovanja**. Plan kontinuiteta poslovanja opisuje način na koji se organizacija priprema za buduće incidente koji bi mogli ugroziti osnovnu poslovnu djelatnost i dugoročnu stabilnost poduzeća. Takvi incidenti uključuju:

- Lokalne incidente (npr. požar, poplava),
- Regionalne incidente (npr. zemljotres) ili
- Nacionalne incidente(npr. pandemija).

U prosincu 2006. godine Britanski institut za standardizaciju izdao je novi standard - BS 25999, koji se naslanja na standarde BS 7799 odnosno ISO/IEC 27001. Taj novi standard proteže se na organizacije svih veličina, vrsta i svrha postojanja, bez obzira na to da li su vladine ili privatne, profitne ili neprofitne, velike ili male, te neovisno o vrsti industrijskog sektora. Dovršeni plan kontinuiteta poslovanja podrazumijeva izdavanje formalnog pisanog priručnika koji mora biti raspoloživ za korištenje prije, tijekom i nakon što je došlo do prekida poslovanja ili katastrofe. Njegova je osnovna svrha umanjiti negativne posljedice po zainteresirane strane, kako po pitanju vrste katastrofe, tako i po pitanju duljine trajanja. Pri tome treba imati na umu da se nazivom “katastrofa” obuhvaćaju svi oblici ekonomskih, građanskih, prirodnih, tehničkih, sekundarnih i posljedičnih incidenata koji imaju negativan utjecaj na poslovanje.

Osnovni dio izrade plana kontinuiteta poslovanja je određivanje ciljnog vremena oporavka (eng. RTO - *Recovery Time Objective*). RTO u biti predstavlja vrijeme unutar kojeg se poslovni procesi moraju ponovno uspostaviti kako bi se izbjegle nepoželjne posljedice povezane s kontinuitetom prekida. RTO se određuje u fazi analize utjecaja (od strane vlasnika procesa), u suradnji s osobom koja izrađuje plan 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 (eng. RTA -*Recovery Time Actual*), dok se razlika do RTO naziva "*gap*". Do stvarne RTA vrijednosti se dolazi simulacijama ili vježbama, odnosno empirijski, u slučaju nastupa stvarnog prekida poslovanja.

Metodologija planiranja kontinuiteta poslovanja mora biti prilagođena svim organizacijama neovisno o veličini i složenosti. Iako ona ima korijene u industrijskom sektoru, svaka organizacija može stvoriti svoj plan kontinuiteta poslovanja. Statistike istraživanja provedenih na Business Continuity Institutu u Velikoj Britaniji(BCI) govore da poduzeća ne ulažu dovoljno vremena i resursa u pripremu plana kontinuiteta poslovanja, pa tako recimo požari rezultiraju zatvaranjem 44% poduzeća u kojima se dogode.

3.2. Izrada plana kontinuiteta poslovnih procesa

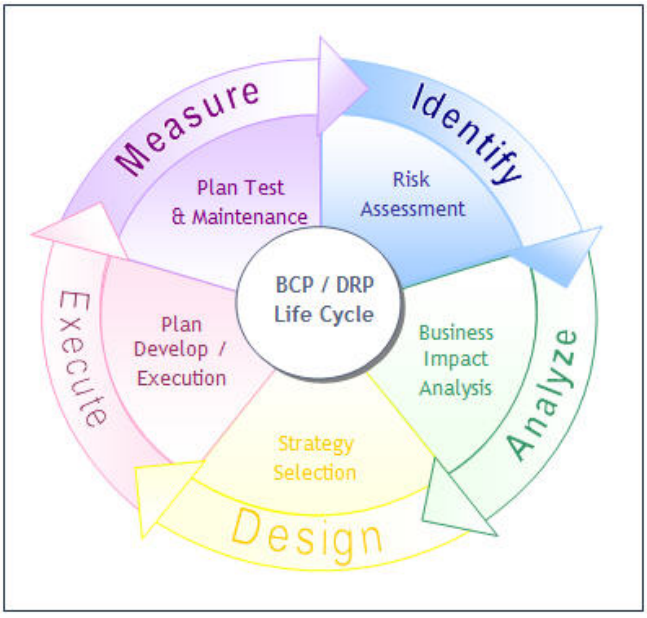
Plan kontinuiteta poslovanja mora biti izrađen tako da bude realističan i da se tijekom krize može koristiti na jednostavan način. Krizno rukovodstvo raspolaže planom kontinuiteta poslovnih procesa te njime upotpunjuje plan oporavka od katastrofe

Osnovne faze izrade plana kontinuiteta poslovanja su sljedeće:

- analiza,
- dizajn rješenja,
- implementacija,
- ispitivanje i prihvaćanje od strane organizacije i
- održavanje prihvaćenog plana.

Institut za kontinuitet poslovanja iz Velike Britanije prikazuje u dijagramu **životne cikluse Plana kontinuiteta poslovanja (**eng. *Life Cycle Business Continuity Planing BCP*, slika 2.) Dijagram prikazuje bitne dijelove vremenskom toku izrade plana. Potrebno je prije svega

- Ustanoviti moguće rizike te utjecaj pojedinih rizika (eng. *Identify, Risk Assessment*),
- Provesti detaljnu analizu utjecaja na posao (eng. *Business Impact Analysis*),
- Dizajnirati rješenje te odabrati strategiju plana oporavka (eng. *Design, Strategy selection*),
- Implementirati dizajn i odabranu strategiju (eng. *Execute, Plan Develop / Execution*) te
- Provesti mjerenja i ispitivanja provedenog plana te održavanje plana u budućnosti (eng. *Measure, Plan Test and Maintenance*)



Slika 2. Životni ciklus Plana kontinuiteta poslovanja
Izvor: Bussiness Continuity Institute UK

Ova lista faza izrade nije definitivna zato što postoji niz čimbenika koje treba uzeti u obzir kod izrade samog plana, odnosno priručnika.

Radi se na primjer o matrici prepoznavanja rizika, to jest točnom definiranju uloga i odgovornosti u planu oporavka poslovanja.

Matrica razine rizika

Razina rizika utvrđuje se množenjem ocjene koja je dodijeljena vjerojatnosti da izvor prijetnje iskoristi ranjivost s ocjenom učinka neželjenog događaja, pri čemu se uzima u obzir prikladnost planiranih ili postojećih kontrola. Tablica 1 daje jednostavan primjer kako se mogu odrediti rizici na temelju podataka o vjerojatnosti da izvor prijetnje iskoristi ranjivost i o učinku.

Primjer u tablici br. 1 jest matrica vjerojatnosti da izvor prijetnje iskoristi ranjivost (veliku, srednju ili malu) i učinka (velikog, srednjeg i malog), koja prikazuje kako se računa ukupna razina rizika.

Na primjer:

- ocjena vjerojatnosti da izvor prijetnje iskoristi ranjivost koja se pripisuje svakoj razini vjerojatnosti prijetnje jest 1,0 za veliku, 0,5 za srednju i 0,1 za malu;
- ocjena učinka koja se dodjeljuje svakoj razini jačine učinka jest 100 za veliku, 50 za srednju i 10 za malu.

Ovisno o potrebama i detaljnosti procjene rizika može se koristiti matrica proizvoljnih dimenzija.

Vjerojatnost da izvor prijetnje iskoristi ranjivost	**Učinak**		
	Mali (10)	Srednji (50)	Veliki (100)
Velika (1,0)	10 x 1,0 = **10**	50 x 1,0 = **50**	
Srednja (0,5)	10 x 0,5 = **5**	50 x 0,5 = **25**	100 x 0,5 = **50**
Mala (0,1)	10 x 0,1 = **1**	50 x 0,1 = **5**	100 x 0,1 = **10**

Tablica 1. Matrica razine rizika
Izvor: Smjernice za upravljanje informacijskim sustavom

Ljestvica rizika

Tablica 2 opisuje razine rizika prikazane u tablici 1. Ljestvica rizika s pripadajućim ocjenama predstavlja stupanj ili razinu rizika kojem su izloženi resursi informacijskog sustava ako je iskorištena određena ranjivost. Stupanj ili razina rizika određuje aktivnosti koje bi se trebale poduzeti.

Razina rizika	**Opis rizika i aktivnosti koje je potrebno poduzeti**
Velik rizik (veći od 51)	Ako je rizik procijenjen kao velik, nužno je hitno provođenje mjera za smanjenje rizika. Postojeći sustav može nastaviti raditi, ali nužno je u što kraćem roku sastaviti plan provođenja mjera te odrediti prioritete i rokove.
Srednji rizik (11 do 50)	Ako je rizik procijenjen kao srednji, nužno je provođenje mjera za smanjenje rizika. Potrebno je sastaviti plan provođenja mjera kako bi se one provele u razumnom vremenu.
Malen rizik (1 do 10)	Ako je rizik procijenjen kao malen, potrebno je utvrditi je li nužno provođenje mjera za smanjenje rizika ili se rizik može prihvatiti.

Tablica 2. Ljestvica rizika i aktivnosti koje je potrebno poduzeti
Izvor: Smjernice za upravljanje informacijskim sustavom

Ostali čimbenici koje je uz matricu prepoznavanja potrebno razmotriti su:

- identifikacija najvećih rizika te strategija njihovog otklanjanja, umanjenja ili transfera te
- detaljni plan promjene lokacije resursa.

Zbog složenosti pristupa i zahtjeva za multidisciplinarnim pristupom, vrlo često se razvoj planova kontinuiteta poslovanja povjerava neovisnim konzultantskim tvrtkama, bez obzira što velike organizacije najčešće posjeduju dobro razvijene odjele informatičke podrške te su u mogućnosti krenuti s razvojem plana i priručnika koristeći vlastite resurse.

3.2.1. Priručnik za kontinuitet poslovanja

Priručnik za kontinuitet poslovanja manje organizacije može biti jednostavan tiskani priručnik koji mora biti spremljen na sigurnom mjestu, udaljenom od primarne radne lokacije. Priručnik treba sadržavati:

1. Imena, adrese i telefonske brojeve kriznog rukovodstva,
2. Listu zaposlenih u generalnim/općim službama,
3. Listu najvažnijih klijenata i dobavljača,
4. Točnu lokaciju udaljenih sigurnosnih kopija podataka,
5. Kopije ugovora o osiguranju te
6. Kopije drugih kritičnih materijala nužnih za ostvarenje kontinuiteta poslovanja organizacije.

Kompleksniji priručnik može sadržavati i sljedeće elemente:

1. Opis sekundarne (rezervne) radne pozicije, u slučaju uništenja ili onesposobljavanja primarne,
2. tehničke zahtjeve poslovanja organizacije,
3. zakonske zahtjeve za izvješćivanjem i akcijama po nastupu katastrofalnog događaja,
4. mjere za početak oporavka radne aktivnosti poduzeća,
5. mjere za ponovno uspostavljanje integriteta fizičkih zapisa,
6. načine ponovnog uspostavljanja lanca nabave i
7. načine izgradnje novih proizvodnih centara.

3.3. Faze planiranja kontinuiteta poslovnih procesa

Osnovne faze izrade plana kontinuiteta poslovanja su sljedeće:

- analiza
- dizajn rješenja
- implementacija
- ispitivanje i prihvaćanje od strane organizacije
- održavanje prihvaćenog plana

3.3.1. Analiza kontinuiteta poslovanja

Faza analize kontinuiteta poslovanja sastoji se od analize utjecaja na poslovanje, analize prijetnji i izrade scenarija utjecaja. Kao rezultat ove faze dobiva se jasna podjela između kritičnih i nekritičnih funkcija u organizaciji.

Poslovna funkcija se smatra kritičnom, ako utjecaj realizacije nekog izvanrednog događaja ima neprihvatljive posljedice po nju i po interese organizacije. Percepcija prihvatljivosti posljedica nastupa izvanrednih događaja može se promijeniti ukoliko se prezentira trošak uspostavljanja i održavanja odgovarajućih poslovnih ili tehničkih rješenja oporavka. S druge strane, određena funkcija može se smatrati kritičnom (ukoliko je takvom definira lokalna zakonska legislativa.)

Analiza utjecaja na poslovanje (eng. *Business Impact Analysis*) je jedan od ključnih koraka u upravljanju kontinuitetom poslovanja. Naime, nije dovoljno samo odrediti rezervnu sigurnu lokaciju i napisati planove oporavka za poslovno kritične funkcije, nego je potrebno odrediti i ciljano vrijeme oporavka. Ciljano vrijeme oporavka je ništa drugo nego maksimalno vrijeme koje si organizacija može priuštiti da joj pojedini ključni poslovni procesi (npr. naplata usluge, interakcija s korisnicima itd.) ne funkcioniraju. Pored toga, potrebno je odrediti međuovisnosti između različitih poslovnih procesa (npr. većina poslovnih procesa ovisi o informatičkoj potpori, što znači da će se taj poslovni proces odnosno funkcija morati prvo oporaviti). Te informacije su bitne iz razloga što

se u sljedećem koraku upravljanja kontinuitetom poslovanja puno jednostavnije može odrediti strategija za nivo opremljenosti rezervne lokacije.

Ako je poslovni proces potrebno oporaviti u iznimno kratkom roku (npr. 4 sata od incidenta), onda će investicija u rezervnu lokaciju biti bitno veća jer će se tada morati unaprijed instalirati sklopovlje, programska oprema, komunikacijski kanali i baze podataka. Ako je poslovni proces takav da je dozvoljeno vrijeme oporavka nešto duže (npr. 4 dana), onda će investicija u rezervnu lokaciju biti puno manja. Razlog tome jest što se tijekom tih 4 dana može nabaviti većina opreme (što znači da se unaprijed ne mora investirati previše novca), uspostaviti komunikacijski kanali i restaurirati programi i baze iz sigurnosnih kopija. Dakle, pažljivo napravljena i odmjerena analiza utjecaja na poslovanje može donijeti velike uštede organizaciji, a da se pri tome ne naruši sigurnost poslovanja.

Tijekom analize utjecaja na poslovanje obično se procjenjuju sljedeći elementi vezani za pojedinu poslovno kritičnu funkciju:

1. Koliko tržišnog udjela organizacija može izgubiti?
2. Kako će klijenti karakterizirati takav prekid poslovanja?
3. Kako će to utjecati na ugled organizacije?
4. Koliko podataka organizacija može izgubiti?
5. Kakve su izravne financijske posljedice (zakonske ili ugovorne kazne)?
6.

Sve te elemente potrebno je promatrati u različitim vremenskim razmacima, i na neki način ih valorizirati. Odrediti prioritet svakog elementa zasebno s obzirom na poslovanje organizacije

Analiza prijetnji

Analiza prijetnji slijedi analizu utjecaja. U ovoj fazi potrebno je identificirati sve potencijalne prijetnje kako bi se detaljno opisali specifični koraci oporavka u slučaju katastrofe. Neke uobičajene prijetnje koje se obrađuju u ovoj fazi su:

- zarazne bolesti,
- zemljotres,
- požar,
- poplava,
- napad preko kompjutorske mreže,
- nestanak struje i vode te
- terorizam.

Sve navedene prijetnje, osim bolesti, dijele zajednički utjecaj na organizaciju, a to je njihov potencijal za oštećivanjem infrastrukture. Utjecaj bolesti usmjeren je primarno na ljudsku komponentu organizacije i može se umanjiti tehničkim i poslovnim rješenjima. Međutim, ukoliko bolesti pogode osobe u organizaciji koje stoje iza provođenja plana oporavka poslovne aktivnosti, primarna zadaća neće biti ispunjena iz razloga što je sudjelovanje rukovodećih osoba u provođenju plana oporavka od neizmjerne važnosti. Rješenje takve ekstremne situacije kao što je bolest rukovodećih osoba u provedbi plana oporavka je samo jako dobro pripravljen plan, spreman podnijeti i najekstremnije situacije.

Scenarij utjecaja

Nakon definiranja potencijalnih prijetnji, potrebno je dokumentirati scenarij utjecaja. Pritom je osnovno pravilo da se planira za katastrofe i događaje vrlo širokog opsega a ne za manje neželjene događaje (pošto su oni redovito sastavni dijelovi većih katastrofa). Po dovršenju faze analize, kao njen izlaz dobiju se dokumentirani poslovni i tehnički planovi zahtjeva. Dobiveni planovi koriste se u fazi implementacije, odnosno provođenja. Provođenje ove faze poprilično je olakšano ukoliko je razvijen dobar sustav rukovođenja imovinom poduzeća (jer on omogućuje laku identifikaciju raspoloživih resursa s informacijama o onima kojima je lagano moguće promijeniti lokaciju). U toj dokumentaciji obično se navodi:

- broj potrebnih radnih mjesta na sekundarnoj lokaciji,

- osobe koje su uključene u proces oporavka zajedno sa podacima potrebnim za kontakt i tehničkim detaljima,
- aplikacije i podaci potrebni za funkcioniranje kritične poslovne funkcije,
- rješenja za privremeno zaobilaženje problema,
- rokovi dozvoljene nedostupnosti poslovnih aplikacija te
- potrebe za uredskim materijalom.

Ovaj plan se odnosi isključivo na uredsku poslovnu okolinu, no i drugi dijelovi poduzeća (odnosno organizacije), poput proizvodnje, distribucije ili skladištenja će morati unutar svog plana oporavka pokriti i ovaj aspekt (povrh onih aspekata koji su specifični za te same poslovne funkcije). Rezultati analize poslovanje često se dokumentiraju kao odvojena strategija kontinuiteta poslovanja.

3.3.2. Dizajn rješenja i implementacija

Cilj faze dizajna je identifikacija troškovno najpovoljnijeg rješenja oporavka od katastrofe koji u sebi pomiruje dva osnovna zahtjeva iz faze analize utjecaja, a to su detaljna analiza prijetnji i analiza mogućih scenarija utjecaja. U fazi dizajna, definirani zahtjevi oporavka i ciljevi oporavka prevode se operativno u konkretne mjere. Najvažniji proizvod ove faze uspostavljanje je organizacije oporavka (eng. *Business Recovery Organization*). Konkretan rezultat uspješnog provođenja ove faze stvaranje je procedura za eskalaciju, obavještavanje i aktivaciju samog plana oporavka s fokusom na kritične poslovne funkcije organizacije.

Tipično, zahtjevi organizacije mogu se izraziti na sljedeći način:

- minimalni zahtjevi za aplikacijama i podacima te
- vremenski rok u kojemu minimalni zahtjevi za aplikacijama i podacima mogu postati opet raspoloživi.

Rezultat faze dizajna rješenja detaljan je opis sljedećih funkcija i aktivnosti:

- zapovjedna struktura kriznog rukovodstva,
- lokacija sekundarnog radnog mjesta (zgrade),
- telekomunikacijska struktura između primarnog i sekundarnog radnog mjesta,
- način replikacije podataka,
- aplikacije i programska podrška koji trebaju biti operativni na sekundarnom radnom mjestu i
- fizički zahtjevi sekundarne radne lokacije.

Faza implementacije

Implementacija je faza u kojoj se elementi dizajna identificirani u fazi dizajniranja provode u djelo. Nju se može promatrati i odvojeno od faze dizajna rješenja no nastavlja se neposredno na nju, i zbog svog operativnog karaktera, predstavlja značajan dio plana kontinuiteta poslovanja kako troškovno, tako i vremenski. Korak izvođenja i implementacije plana kontinuiteta poslovanja u pravilu ne može biti uspješan ukoliko nije uspostavljen centar ili odbor za izvođenje hitnih akcija, te ukoliko u prethodnim fazama nisu adekvatno definirane procedure za nastavak rada, oporavka i obnavljanja svih nužnih poslovnih resursa. Za većinu organizacija je značajan i sustav održavanja te stalna procjena ugovora s vanjskim dobavljačima, te održavanje kontingentnih rezervi svih kritičnih resursa. Naposljetku, u fazi implementacije započinje se s internim kampanjama o važnosti praćenja procedura vezanih uz stvaranje plana kontinuiteta i oporavka, te treningom, kako svih izravno uključenih u akcije oporavka, tako i svih korisnika usluga poslovnog sustava.

3.3.3. Ispitivanje i prihvaćanje od strane organizacije

Svrha ispitivanja je postizanje prihvatljivosti plana poslovnog kontinuiteta od strane organizacije, odnosno sukladnosti sa svim zahtjevima koje pred plan poslovnog kontinuiteta postavlja uprava poduzeća.

Planovi mogu biti i neuspješni u odnosu na očekivanja zbog nedovoljnih ili netočno predviđenih mjera oporavka, grešaka u dizajnu ili primjeni rješenja.

Testiranje može uključivati sljedeće faze:

1. testiranje poziva kriznog tima za upravljanje,
2. tehnički test prelaska s primarne na sekundarnu lokaciju,
3. tehnički test prelaska sa sekundarne na primarnu lokaciju,
4. test aplikacija i
5. test poslovnih procesa.

U pravilu, ispitivanje se provodi najmanje svake dvije godine. Problemi identificirani tijekom inicijalne test faze mogu se prenijeti u fazu održavanja plana i mogu se iznova ispitivati tijekom sljedećeg ciklusa testiranja. Pri prihvaćanju plana poslovnog kontinuiteta, potrebno je izvršiti procjenu da li uvođenje mjera predviđenih planom kontinuiteta poslovanja predstavlja prikladan odgovor na moguće rizike.

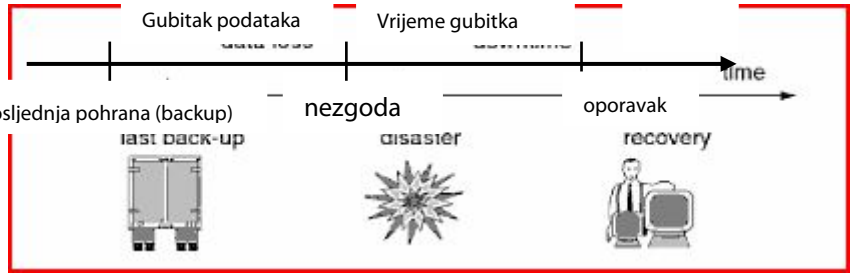
No, osim čiste tehničke prihvatljivosti mjera oporavka, nužno je da su one sukladne ciljevima, politikama i etičkim stavovima organizacije. Tako npr. neka mjera oporavka može biti cjenovno prihvatljiva organizaciji (npr. premještanje poslovanja na sekundarnu lokaciju koja je udaljena 100 km od mjesta gdje živi većina zaposlenika i nalazi se u ruralnom, prometno slabo povezanom području), ali ne i zaposlenima. Neka mjera oporavka, iako je vrlo učinkovita (npr. prigodna lokacija za povrat podataka i ponovnu uspostavu servisa i usluga) može biti previše skupa i samim time neće biti prihvatljiva za one koji imaju financijski interes ili ulog u poslovanju organizacije. Naposljetku, često se u praksi događa, osobito u financijskom i bankovnom sektoru, da je neka mjera oporavka prihvatljiva organizaciji po svim promatranim kriterijima, ali nije u skladu sa zakonskim propisima, odnosno legislativa zahtijeva dodatne mjere.

Prema tome, pri prihvaćanju mjera određenih planom potrebno je u mjerljivim jedinicama izraziti koje su mjere oporavka prihvatljive svim uključenim stranama: ulagačima, organizaciji, zakonodavcu i klijentima organizacije.

Pri prihvatu mjera plana oporavka koriste se neki ili svi od navedenih kriterija:

1. Jesu li svi kriteriji prihvata kvantitativno mjerljivi?
2. Da li je postizanje mjera oporavka pod zadanim uvjetima realistično?
3. Da li je grupiranje kriterija realistično, tj. da li su kriteriji prihvata u konfliktu?
4. Da li su uzeti u obzir svi kriteriji prihvata koji bi činili plan oporavka kompletnim?

Andrew Hiles u knjizi *„Definitive Handbook of Business Continuity Management“* između ostalog opisuje i tok oporavka u informatičkom sektoru (Slika 3.) prikazujući neizbježnu važnost posljednje sigurnosne kopije podataka. Naime, vrijeme proteklo od posljednje kopije i nezgode je vrijeme nepovratnog gubitka podataka.



Slika 3 Tok oporavka Informatičkog sektora
Izvor: The Definitive Handbook of Business Continuity Management

U pravilu, kvantitativni pokazatelji koje se može koristiti pri procjeni prihvata su (neki ili svi od navedenih):

1. Točno vrijeme, datum i sat oporavka pojedinih funkcija.
2. Dozvoljeno trajanje vremena prekida usluge.
3. Minimalno osoblje potrebno za ponovno uspostavljanje usluge na određenom nivou.
4. Nivo funkcionalnosti usluge koja se ponovno uspostavlja.
5. Kapaciteti potrebni za ponovno uspostavljanje usluge.
6. Trošak razvoja sekundarnih kapaciteta ili oporavka pojedine usluge.
7. Trošak održavanja sekundarnih kapaciteta potrebnih za oporavak.

Primjena navedenih kriterija i pokazatelja omogućavaju planu za upravljanje kontinuitetom poslovnih procesa da pomiri tehničku uspješnost projekta s očekivanjima svih uključenih strana, odnosno onih koji imaju svoj interes u uspješnom kontinuitetu poslovanja i postojanja neke organizacije. Na taj način moguće je objektivno sagledati budući uspjeh uvođenja plana kontinuiteta poslovanja u odnosu prema mjerljivim kriterijima koji se uspostavljaju neposredno na početku izrade plana.

3.3.4. Održavanje prihvaćenog plana

Održavanje priručnika za kontinuitet poslovanja dijeli se u tri periodične aktivnosti. Prva aktivnost je potvrda informacija u priručniku, distribucija svim zaposlenima na uvid i specifični trening za zaposlenike koji su kritični za plan i oporavak. Druga aktivnost je testiranje i provjera tehničkih rješenja za provođenje operacije oporavka. Treća aktivnost je testiranje i provjera dokumentiranih procedura oporavka koja se tipično radi jednom godišnje ili jednom u dvije godine. Pošto se sve organizacije mijenjaju tijekom vremena, priručnik kontinuiteta poslovanja mora se mijenjati kako bi ostao relevantan za organizaciju.

Neki podaci koje je potrebno identificirati i osvježavati unutar plana su:

- promjene u rasporedu zaposlenika,
- promjene po pitanju ključnih klijenata i njihovi kontakt podaci te
- promjene odjela unutar poduzeća ili organizacije (poput otvaranja novog odjela, zatvaranja postojećeg odjela ili fundamentalnih organizacijskih promjena).

Kao dio tekućeg održavanja, svako tehničko rješenje mora imati provjerenu funkcionalnost. Tipične akcije su provjera distribucije novih virusnih definicija, sigurnost aplikacija, distribucija sigurnosnih zakrpa, provjera operativnosti sklopovlja i aplikacija te provjera sigurnosti podataka. Pošto se poslovni procesi mijenjaju tijekom vremena, organizacijske procedure oporavka iz prošlosti mogu postati neadekvatne. Tipične provjere uključuju:

- provjeru da li su radni procesi kritičnih poslovnih funkcija dokumentirani,
- da li su se sustavi uključeni u izvođenje kritičnih funkcija promijenili,
- da li su dokumentirane radne liste provjera smislene i točne te
- da li dokumentirane procedure oporavka i potporna infrastruktura tijekom oporavka od katastrofe omogućuju oporavak unutar unaprijed određenog vremena.

Povezanost s ostalim fazama u upravljanju kontinuitetom poslovanja

Postoji direktna povezanost između testne faze, faze održavanja i faze analize utjecaja. Kod uspostavljanja priručnika upravljanja kontinuitetom poslovanja i inicijalnog podizanja infrastrukture oporavka, nedostaci otkriveni tijekom testne faze moraju biti ulazni parametar ponovnog odvijanja faze analize utjecaja.

Faza održavanja značajna je po tome što predstavlja fazu u kojoj se, osim konkretne implementacije, odvija najveći dio konkretnih, operativnih i tehničkih aktivnosti. Ovo je faza za čiju je uspješnost nužno uključivanje specijalista iz područja raznih informatičkih disciplina te njihova uska suradnja s vanjskih konzultantima uključenima u izgradnju integralnog informacijskog i poslovnog sustava poduzeća (ukoliko takvo osoblje nije na raspolaganju unutar organizacije).

U ovoj fazi često se provjerava distribucija antivirusnih definicija, provjera integriteta podataka, provjera funkcionalnosti programske podrške, funkcionalnost poslovnih aplikacija (osobito njihove jezgre) te sigurnosti aplikacija i distribucije sigurnosnih zakrpa. Međutim, u ovoj fazi se testiraju i procedure oporavka, njihova dokumentiranost, jasnoća razgraničenja funkcija u procesu samog oporavka te da li se postižu unaprijed definirana vremena oporavka. Važno je fazu održavanja plana kontinuiteta poslovanja povezati s upravljanjem promjenama pošto se svaka promjena poslovnog sustava reflektira na predviđene procedure oporavka i rezultira novim informacijama i potrebnim akcijama za obnavljanje plana oporavka.

Sastavni dio ispitivanja, ali i održavanja plana kontinuiteta poslovanja je testiranje funkcionalnosti rezervnih kapaciteta. Neke organizacije preferiraju pri testiranju rezervnih lokacija neko vrijeme na njima voditi kompletno poslovanje (pa vratiti na primarnu lokaciju) kako bi se osigurale da je funkcionalnost obje lokacije potpuna.

Postavlja se pitanje koliko je često potrebno provoditi reviziju plana kontinuiteta poslovnih procesa. Odgovor ovisi o tome koliko su česte organizacijske promjene. Dobro je pravilo da neovisno o promjenama, tim zadužen za izradu plana treba provoditi kvartalne, regularne promjene, no suštinske promjene mogu biti i češće i rjeđe, ovisno o prirodi promjena unutar organizacije. Isto tako, plan kontinuiteta poslovnih procesa može biti napravljen na robustan način, tako da može prihvatiti (bez većih zahvata nad sustavom) veću količinu promjena.

4. Ljudski resursi u kontinuitetu poslovanja

Osnovna snaga organizacije su ljudi. Zato ključ krajnjeg uspjeha leži u načinu na koji tvrtke odabiru i organiziraju ljude, to jest kako upravljaju ljudskim resursima. Ljudi imaju svoju vlastitu volju, svoje vlastite želje i svoj način razmišljanja. Ako zaposlenici nisu sami dovoljno motivirani da bi postigli ciljeve rasta i tehnološkog razvoja, jednostavno neće biti ni rasta, ni povećanja produktivnosti, a tako ni tehnološkog razvoja organizacije.

Ako se ljude uključi aktivno u promjene te osjete da su bitni i da pridonose svojim radom , oni će tome dati svoju podršku. To posebno vrijedi za upravljanje kontinuitetom poslovnih procesa. Svi zaposlenici trebaju imati osnovno razumijevanje principa upravljanja kontinuitetom poslovnih procesa i njihov značaj za organizaciju. Zaposlenici bi također trebali biti aktivno uključeni u proces planiranja za vlastite poslovne jedinice. Ako je uprava organizacije zabrinuta da će upravljanje kontinuitetom poslovanja BCM (eng. *Business Continuity Management*) zaposlenici promatrati kao još jedan kratkoročni trend, koji kao posljedicu neće dugo zadržati interes osoblja, potrebno je osigurati da svi zaposlenici organizacije budu uključeni u razvoj plana za upravljanje kontinuitetom poslovanja.

4.1. Treniranje osoblja i podizanje svijesti

Tim za upravljanje kontinuitetom poslovnih procesa koji planira i provodi potrebne promjene, mora ostvariti zadovoljavajući nivo komunikacije sa zaposlenicima, objasniti im uzroke i svrhu promjena. Ponekad je prvi korak osvještavanje ljudi o potrebi za upravljanje kontinuitetom poslovanja. Potrebna je edukacija i informiranost zaposlenika o prednostima tog plana za poslovanje organizacije, posebice u neplaniranim događajima koji mogu zadesiti organizaciju.

Osim edukacije, zaposlenike je potrebno motivirati kako bi ih se potaklo da ulože više truda i interesa u provedbu plana kontinuiteta poslovanja.

Motivirati ih se može:

- većom slobodom u odlučivanju o metodama rada, redoslijedu i brzini obavljanja radnji poticanjem participacije i interakcije među zaposlenicima,
- davanjem osjećaja osobne odgovornosti za izvršenje zadatka i
- povratnom informacijom o postignuću radnika uključivanjem u analizu i promjenu radnog okruženja.

Motivirani član tima obično je energičan i pun oduševljenja, trajno dobro radi i aktivno nastoji dobiti šire nadležnosti. Takvog pojedinca ne plaši mogućnost promjene i pozitivno pristupa izazovima. Visoko motivirani član tima može pomoći u podizanju morala ostatku tima i povući ga ka većim postignućima. Prethodno navedene odlike motiviranog člana tima su od izuzetne važnosti u slučajevima katastrofa ili svakodnevnih neplaniranih nezgoda na poslovnom planu organizacije. S druge strane, nemotivirani član tima često će se doimati nezainteresiranim za postavljene zadatke i ciljeve, a samim time u dogledno vrijeme još otežati provođenje plana.

Uključenost djelatnika, odnosno zaposlenika na svim razinama tvrtke je od izuzetne važnosti. Svaki djelatnik je odgovoran za svoj rad, ali pravilno motiviran i educiran djelatnik spreman je preuzeti odgovornost za cijeli tim, pa čak i na globalnoj razini organizacije. To je ključno za uspjeh provođenja plana upravljanja kontinuitetom poslovanja. Međudjelovanje vodstva i radnika, kao i naglašavanje timskog rada, povećava uspjeh te potiče globalnu svijest unutar organizacije.

5. Zaključak

Planiranje kontinuiteta poslovanja je na prvi pogled skup i složen proces s upitnim rezultatima. Jednostavnije je ne činiti ništa i nadati se da će se nezgoda dogoditi nekome drugom. Za izradu učinkovitog plana potreban je angažman svih jedinica organizacije. Kod velikih organizacija to je dugotrajan kružni proces sa stalnim revizijama i nadopunama.

No unatoč cijeni i potrebnim resursima, u današnjem vremenu kompanije sve više i više shvaćaju da je potrebno odgovoriti na prijetnje neželjenih događaja. Počevši od ekstrema poput terorizma, prirodnih katastrofa, ali i svakodnevnih nezgoda poput dugotrajnijih gubitaka struje, pada telefonske i Internet veze itd. Odgovor je planiranje kontinuiteta poslovanja, jedina korisna metodologija nužna za optimalno poslovanje u ekstremnim uvjetima. Neovisno o razlogu (priprema kompanije za europsku legislativu, smanjenje štete u slučaju nezgode, ubrzana reakcija kompanije na nezgodu i sl.) uvođenje plana kontinuiteta poslovanja u kompanije, bez obzira na veličinu i cijenu, ekonomski je racionalna odluka.

Zbog konstantnih promjena poslovnih zahtjeva, tehnike planiranja poslovnog kontinuiteta koje su bile adekvatne prije više godina, u današnje doba postaju zastarjele. Iako temeljne postavke ostaju, moderni planovi kontinuiteta poslovanja moraju biti fleksibilni i moraju inzistirati na prevenciji, a ne isključivo se baviti rješavanjem već nastalih problema. Planiranje mora biti fleksibilno na način da daje opće okvire, a ne orijentira se samo na identificirane prijetnje. Sve učestalije prirodne katastrofe i teroristički napadi na globalnoj razini priuštili su svim velikim organizacijama upozorenje da ako žele biti trajno konkurentni moraju biti spremni i na neočekivano.

6. Reference

[1] Business Continuity Planning *Planning for cost-effective recovery and resiliency* http://www.metricstream.com/solution_briefs/BCP_FFIEC_Compliance.htm.

[2] Andrew Hiles: The Definitive Handbook of Business Continuity Management, John Wiley and Sons, 2007

[3] Network intelligence an ISO 27001 Company, Business Continuity Management consulting http://www.niiconsulting.com/services/bcm/Business_Continuity_Management.html

[4] Wikipedia : http://en.wikipedia.org/wiki/Business_continuity_planning

[5] Portal za informacijsku sigurnost : http://www.sigurnost.info/

[6] Istraživanja instituta za upravljanje kontinuitetom poslovanja: http://www.thebci.org/BCIResearchReport.pdf

[7] Implementacija sustava za upravljanje kontinuitetom poslovanja, King ICT, Hrvatska http://www.king-ict.hr/Default.aspx?tabid=757