Centar Informacijske Sigurnosti

Upravljanje kontinuitetom poslovnih procesa

lipanj 2011.

CIS-DOC-2011-06-017

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

Prekidi u odvijanju poslovnih procesa mogu tvrtkama nanijeti ozbiljne financijske gubitke. Ti gubici mogu biti vidljivi, odnosno mjerljivi, odmah, ali mogu biti i trenutno zanemarivi ili neprimjetni. Ipak, mogu se dugoročno pokazati presudnima za poslovanje tvrtke. Prekid u poslovanju, koliko god kratak bio, na današnjem kompetitivnom tržištu, može dovesti do pada vjerodostojnosti tvrtke u očima klijenata, odnosno gubitka ugleda tvrtke. Tako dolazi do dugoročnih financijskih gubitaka koji nisu vidljivi odmah, ali se na kraju mogu pokazati odlučujućima.

Planiranje odnosno upravljanje kontinuitetom poslovnih procesa (eng. *Business continuity planning,* BCP ili *Business continuity management,* BCM) je proces izrade i dorade logističkog plana koji daje smjernice kako izbjeći, ublažiti, te u slučaju najgoreg, oporaviti se, odnosno ponovno pokrenuti poslovanje, nakon kraha uzrokovanog nezgodom. Neke od tih nezgoda mogu biti poplave, požari, pandemije ili epidemije zaraznih bolesti i slične prirodne sile. U drugu vrstu događaja sa znatnim utjecajem na poslovanje tvrtke spadaju, na primjer, gubitak dobavljača sirovina na kojima se zasniva poslovanje tvrtke, kvarovi informatičke i mrežne opreme nužne za vođenje poslovnih procesa, ili gubitak važnih podataka uzrokovan zarazom računala zlonamjernim programima. Također, ne treba zanemariti niti krađe ili uništavanje opreme, odnosno vandalizam.

Rizici od navedenih nezgoda nisu za sve tvrtke jednaki pa tako ni logistički plan kako ih izbjeći odnosno ublažiti jednom kad se dogode nije za sve tvrtke isti. Iz istog razloga složenost izrade i dorade, odnosno osvježavanja plana da bude u skladu s promjenama u tvrtki i poslovanju nije jednaka. Međutim, ono što je zajedničko svim vrstama nezgoda - financijska šteta, stvarna je opasnost za sve tvrtke. Mogući financijski gubici se lako izračunaju, samo se uzme u obzir gubitak nekog poslovnog procesa odnosno odjela u tvrtki, gubitak neke sirovine odnosno njenog dobavljača ili dijela opreme te se pretpostavi neki vremenski period da se taj dio poslovanja ponovno uspostavi. Tada se lako vidi koliko je ustvari važno imati dobar plan za izbjegavanje odnosno ublažavanje i skraćivanje takvih situacija.

Ovaj dokument opisuje najvažnije elemente upravljanja kontinuitetom poslovnih procesa, od same analize poslovanja prije donošenja logističkog plana za upravljanje poslovnim procesima, preko edukacije djelatnika, do osuvremenjivanja odnosno prilagodbe samog plana promjenama u tvrtki i poslovnim procesima koje koristi.

2. Identifikacija mogućih prijetnji i analiza rizika

Standard BS 25999, donesen u Velikoj Britaniji krajem 2006. godine, je prvi pokušaj da se propiše procedura i sveobuhvatnost upravljanja kontinuitetom poslovnih procesa za tvrtke raznih veličina i područja poslovanja. Taj standard obuhvaća organizacije svih veličina, vrsta i svrha postojanja, bez obzira na to jesu li 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 zbog nezgode.

Za donošenje logističkog plana odnosno priručnika za upravljanje poslovnim procesima tvrtke prilikom događaja koji mogu negativno utjecati na poslovanje, treba proći kroz nekoliko ključnih radnji. Odnosno u ciklusima treba prolaziti redovito kroz te radnje kako bi plan bio u skladu s promjenama u poslovanju tvrtke, ali i na tržištu, te tako ostao učinkovit. Te radnje, prikazane na Slika 1, su:

1. analiza poslovanja,
2. izrada rješenja,
3. provedba rješenja,
4. provjera rješenja i prilagodba rješenja promjenama.

Navedene radnje opisane su narednim podpoglavljima.

Slika 1. *Faze donošenja i prilagodbe plana*
Izvor: *LSS*

2.1. Analiza

Faza analize poslovanja, te analize utjecaja nepoželjnih događaja na poslovanje, temelj je kvalitetnog i cjelovitog plana za upravljanje kontinuitetom poslovanja. Tek prilikom provođenja metoda za upravljanje kontinuitetom poslovnih procesa, mnogi zaposlenici, čak i voditelji nekih poslovnih procesa, prvi puta steknu uvid u cjelokupno poslovanje tvrtke i razumijevanje povezanosti različitih poslovnih procesa i njihov međusobni utjecaj. Ovo se prije svega odnosi na fazu analize.

2.1.1. Analiza utjecaja

Rezultat analize utjecaja jest podjela poslovnih i organizacijskih procesa na ključne i periferne, odnosno identifikacija ključnih procesa za uspješno poslovanje tvrtke. To su poslovni procesi koje treba u najkraćem mogućem roku ponovno uspostaviti u slučaju prekida poslovanja. Ključni procesi se mogu definirati kao oni čiji je gubitak neprihvatljiv za poslovanje tvrtke. Gubitak poslovnog procesa može biti neprihvatljiv s financijskog stanovišta, a sama percepcija prihvatljivosti gubitka poslovnog procesa može se promijeniti nakon analize kada se ustanovi trošak uspostavljanja i održavanja odgovarajućih poslovnih ili tehničkih rješenja oporavka. S druge strane moguće je i da su neki dijelovi poslovanja propisani zakonom. U tom slučaju i oni se smatraju ključnima zato što njihovim prekidom prijete pravne mjere, a samim time i dodatni financijski odnosno pravni troškovi.

Svakom ključnom poslovnom i/ili organizacijskom procesu dodjeljuju se dvije vrijednosti:

- **RPO (eng. *Recovery Point Objective*):** je ciljana količina podataka koje je potrebno povratiti nakon nezgode, odnosno ciljani period poslovanja iz kojeg je potrebno povratiti poslovne podatke.
- **RTO (eng. *Recovery Time Objective*):** je ciljana količina vremena potrebnog za ponovno pokretanje određenog poslovnog i/ili organizacijskog procesa odnosno prikupljanje količine podataka navedenih u RPO.

Ovisno o RPO-u (i RTO-u) bira se najučinkovitija metoda izrade sigurnosnih kopija.

1. **primjer:** Tvrtka posluje većinom s istim klijentima te nema potrebu za čestim sigurnosnim pohranama financijskih i kontakt podataka. Njezin RPO bi mogao biti jedan tjedan, odnosno bitni podaci za poslovanje te tvrtke su najviše jedan tjedan stari. RTO takve tvrtke može biti do 24 sata odnosno u slučaju prekida poslovanja i gubitka podataka tvrtka želi ponovno uspostaviti poslovanje i vratiti podatke iz sigurnosnih kopija za 24 sata. Za takvu tvrtku pohrana sigurnosnih kopija na eksternom čvrstom disku ili nekoliko njih, koji se ovisno o vrstama prijetnji na mjesto poslovanja mogu čuvati na udaljenom mjestu, je sasvim prihvatljiva, dovoljna i isplativa metoda izrade sigurnosnih kopija.
2. **primjer:** Tvrtka posluje s klijentima čiji se kontakt podaci mijenjaju često i/ili sama vodi svoje financijske podatke, kao na primjer neka financijska kuća. Analizom svog poslovanja, takva tvrtka može doći do RPO vrijednosti od 0, odnosno važni podaci za njeno poslovanje se stvaraju ili mijenjaju svakog trenutka. Često takve tvrtke imaju i nizak RTO, odnosno u svrhu uspješnog nastavka poslovanja trebaju te podatke odmah. Recimo da je RTO jedan sat odnosno da u slučaju nezgode i gubitka podataka tvrtka želi izgubiti najviše sat vremena prije nego nastavi s daljnjim poslovanjem. Najbolji način sigurnosne pohrane podataka bi bila mrežna pohrana u realnom vremenu koja ovisno o prijetnjama na mjesto poslovanja može biti udaljena.

Ova dva primjera mogu se smatrati rubnim slučajevima, odnosno primjerima gdje je RPO jako visok ili jako nizak. Neke tvrtke tako mogu najviše izgubiti podatke iz proteklih par sati, a da značajno ne utječu na uspješan nastavak poslovanja. Kod njih je RPO, na primjer, 8 sati. Najčešće su RPO i RTO povezani, što se može vidjeti i na navedenim primjerima. Tvrtke koje imaju potrebu za visokim postotkom povrata izgubljenih podataka imaju potrebu za tim podacima prije odnosno brže trebaju te podatke natrag da bi nastavile sa poslovanjem. Međutim to nije pravilo i zato je najisplativija metoda sigurnosne pohrane individualna stvar i potrebno je pristupiti analizi poslovanja.

Provođenje i praćenje RPO-a nakon prekida poslovanja osigurava da se ne prekorači najveći dozvoljen gubitak podataka - MTDL (eng. *Maximum Tolerable Data Loss*), dok provođenje RTO-a osigurava da se ne prekorači vremenski period dozvoljen za ponovno uspostavljanje određenog procesa - MTPD (eng. *Maximum Tolerable Period of Disruption*). MTDL i MTPD su doneseni kao vrijednosti čije prekoračivanje bi vjerojatno značilo kraj poslovanja za tvrtku, odnosno nemogućnost uspješnog oporavka od nezgode i nastavak poslovanja.

2.1.2. Analiza prijetnji poslovanju

Analiza i dokumentiranje mogućih prijetnji potrebni su kako bi se mogli uspostaviti koraci prema ponovnoj uspostavi poslovanja specifični svakoj prijetnji. Prijetnje uspješnom poslovanju najčešće se dijele na prijetnje iz okoline, namjerne štete, gubitak sirovina i kvarove opreme nužne za poslovanje.

Neke uobičajene prijetnje, ovisno o vrsti djelatnosti koje tvrtka obavlja i samom mjestu poslovanja, su:

- potresi,
- poplave,
- požari,
- bolest djelatnika odnosno epidemija,
- napadi na IT sustave,
- sabotaža poslovanja,
- krađa opreme, novca ili podataka,
- prekid napajanja električnom energijom,
- gubitak dobavljača odnosno sirovina nužnih za proizvodnju,
- kvar informacijske i/ili komunikacijske opreme te
- kvar na proizvodnim strojevima.

2.1.3. Procjena rizika za poslovanje

Nakon analize mogućih prijetnji poslovanju zapisuju se vjerojatnosti događanja te utjecaj na poslovanje ukoliko dođe do nesretnog događaja. Do tih vjerojatnosti moguće je doći istraživanjem učestalosti sličnih događaja u prošlosti. U slučaju prirodnih katastrofa može se istražiti njihova povijest na mjestu poslovanja. Dok se u slučaju sabotaža i krađa, uz istraživanje mjesta odnosno zajednice u kojoj je poslovna zgrada, može pristupiti i istraživanju sličnih događaja u samoj tvrtki te pratiti njihov trend odnosno učestalost. Takva procjena rizika može se bilježiti u tablici kao što je sljedeća.

OPIS DOGAĐAJA	VJEROJATNOST DOGAĐAJA	UTJECAJ NA POSLOVANJE
Poplava	Niska	Velik
Sabotaža	Niska	Vrlo velik
Krađa	Visoka	Srednji

Tablica 1. *Procjena rizika u poslovanju*

Skala vrijednosti za vjerojatnost događaja može biti izražena na sljedeći način:

1. vrlo niska,
2. niska,
3. srednja,
4. visoka i
5. vrlo visoka vjerojatnost nesretnog događaja.

Dok skala vrijednosti za utjecaj događaja na poslovanje može biti opisana vrijednostima kao što su:

1. vrlo malen,
2. malen,
3. srednji,
4. velik i
5. vrlo velik utjecaj nesretnog događaja na poslovanje.

Međutim, skala može biti i brojčana s istim vrijednostima kao prije, ali izražena brojevima od 1 do 5 ili po potrebi i preciznijom granulacijom (npr. od 1 do 10 ili više). Ovakva tablica donosi dodatan uvid u rizike za poslovne procese. Primjer Tablice 1 sa brojčanim vrijednostima:

OPIS DOGAĐAJA	VJEROJATNOST DOGAĐAJA	UTJECAJ NA POSLOVANJE	STUPANJ RIZIKA
Poplava	2	4	8
Sabotaža	2	5	10
Krađa	4	3	12

Tablica 2. *Procjena najvećeg rizika za poslovanje*

U takvoj tablici moguće je izračunati razine rizika jednostavnim množenjem vjerojatnosti događanja nekog nesretnog događaja i razine njegovog utjecaja na poslovanje i poslovne procese tvrtke. Veća brojčana vrijednost u polju „STUPANJ RIZIKA“ označava rizike kojima treba posvetiti pažnju prije onih s manjim ukupnim stupnjem rizika.

3. Izrada plana

Nakon analize poslovanja i rizika za poslovanje, te uspješne identifikacije najvećih rizika, slijedi pokušaj da se oni umanje ili čak otklone. Ovo je važna faza u upravljanju kontinuitetom poslovnih procesa jer donosi iznova novi uvid u poslovanje tvrtke i promjene u strategiji upravljanja poslovnim procesima. Rizici se umanjuju svim dostupnim metodama, ovisno o isplativosti, od tehničkih rješenja do promjena mjesta poslovanja.

Nakon usvajanja strategije za smanjenje rizika slijedi izrada logističkog plana za upravljanje kontinuitetom poslovnih procesa, odnosno dokumentiranje koraka koje je potrebno proći u slučaju nezgode te načina kako osigurati što brži oporavak poslovanja. Prema podacima dobivenim analizom poslovanja i rizika za tvrtku izrađuje se priručnik za djelovanje u slučaju nezgode i potrebe za ponovnim pokretanjem poslovanja ili nekih poslovnih procesa.

Ovisno o potrebama tvrtke i njenom poslovanju, priručnik sadrži:

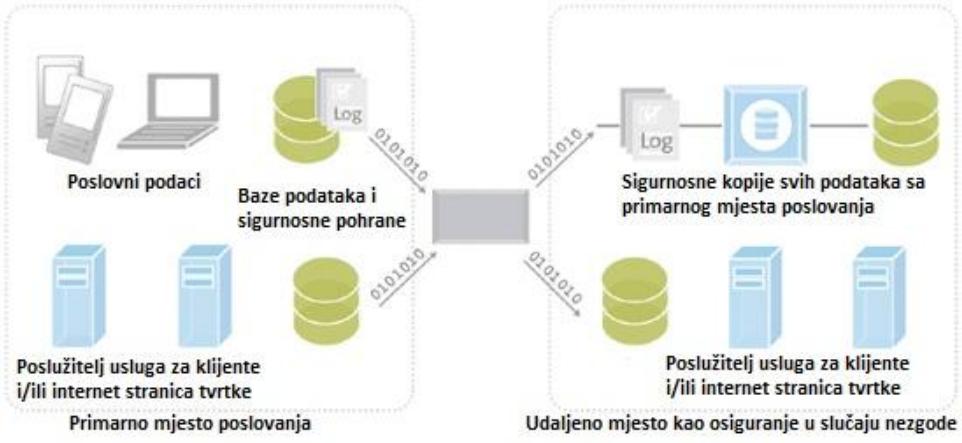
- imena, adrese i telefonske brojeve tima za upravljanje,
- listu najvažnijih klijenata i dobavljača,
- točnu adresu udaljenih sigurnosnih kopija podataka,
- kopije ugovora sa osiguravajućim kućama,
- kopije drugih nužnih materijala za ostvarenje kontinuiteta poslovanja tvrtke.

U većim i složenijim organizacijama plan može sadržavati i adresu sekundarnog prostora za obavljanje djelatnosti u slučaju uništenja primarnog te najmanju količinu opreme i/ili sirovina potrebnih za poslovanje tvrtke. Prema tome, plan većih organizacija sadrži:

- adresu sekundarnog radnog prostora,
- broj radnih stolova,
- broj računala,
- materijale za pisanje (papiri i olovke) te
- kopiju podataka nužnih za poslovanje.

Ti materijali, nužni za poslovanje, mogu već biti kupljeni i pohranjeni na sekundarnom radnom mjestu, ali najčešće, zbog financijskih razloga mogu biti navedene samo adrese i kontakt podaci nekoliko različitih dobavljača takvog materijala koji se može kupiti u slučaju nesretnog događaja.

Prilikom nesretnih događaja svih vrsta, jedan od najvećih rizika za tvrtku je gubitak podataka. Iz tog razloga jedan od važnih koraka upravljanja kontinuitetom poslovnih procesa je izrada sigurnosnih kopija tih podataka. A način kako doći do tih podataka je jedna od važnijih stavki u logističkom planu za ponovnu uspostavu poslovanja.



Slika 2. *Sigurnosna pohrana podataka na udaljenom mjestu*
Izvor: *LSS*

3.1. Učinkovit plan

Jedna od značajki dobrog plana za upravljanje kontinuitetom poslovnih procesa jest njegova učinkovitost, odnosno omjer cijene i količine zaštite koju pruža tvrtci. Između te dvije, najčešće nepomirljive, odrednice plana traži se kompromis, to jest da rješenje ne bude preskupo za provođenje, ali da pokriva sve ključne poslovne procese te nužnu opremu i sirovine za odvijanje poslovnih procesa. Naravno, prilikom izrade plana i donošenja kompromisa treba paziti da se ne prekorače već spomenuti parametri MTDL i MTPD (opisano u poglavlju 2.1.1).

3.2. Smjernice za uspostavu poslovanja

Ovisno o vrsti rizika, odnosno vjerojatnosti pojedinog nesretnog događaja, donose se smjernice za reakciju nakon prekida poslovanja koje sačinjavaju ključan dio plana. To su koraci koje je potrebno proći u slučaju nezgode te na taj način osigurati što brži oporavak poslovanja. Preporuča se donošenje plana za što veću odnosno sveobuhvatniju prijetnju poslovanju. Takav plan pokriva i niz manjih nezgoda te poteškoća koje tvrtka treba riješiti za ponovno pokretanje poslovanja, a uvijek se može koristiti djelomično u slučaju manje nezgode za ponovno pokretanje samo djela poslovnih procesa. Na primjer, plan koji navodi smjernice za uspostavu poslovanja nakon teške poplave može sadržavati i smjernice kako ponovno uspostaviti poslovne procese nakon:

- prekida u napajanju električnom energijom,
- uništenja odnosno gubitka informacijske i komunikacijske opreme,
- gubitka lokalnih dobavljača sirovina potrebnih za proizvodnju te
- gubitka strojeva za proizvodnju.

3.3. Uspostava tima za upravljanje

Prilikom izrade plana potrebno je dokumentirati imena i kontakte pojedinaca uključenih u proces ponovne uspostave poslovanja, odnosno način kako doći do njih u slučaju nezgode i područja poslovanja tvrtke za koja su zaduženi. Oni sačinjavaju tim za upravljanje i donošenje odluka u slučaju nezgode, a predstavljaju i ključne osobe za provjeravanje i promjene plana za ponovnu uspostavu poslovanja. Tim za upravljanje je najčešće sastavljen od osoba na odgovornim pozicijama koje imaju dobar uvid u poslovanje tvrtke te su vrlo vjerojatno sudjelovale u samoj fazi analize poslovanja. Kako je upravljanje kontinuitetom poslovanja u današnje vrijeme sve više povezano s računalnim i informacijskim sustavima, što zbog načina kako se moderni poslovni procesi izvode, što zbog sve zastupljenije digitalizacije svih poslovnih podataka, u tima za upravljanje se nalazi barem jedan IT stručnjak.

4. Provođenje plana

Provođenje plana je treća faza (poglavlje 3) u kojoj se u suštini prate i provode smjernice za ponovnu uspostavu poslovanja koje se nalaze u samom logističkom planu odnosno priručniku u slučaju nezgode. Plan je potrebno povremeno provesti iz jednostavnog razloga njegove provjere. Ovisno o veličini tvrtke, složenosti poslovanja, ali i riziku za poslovanje uspostavljenom u fazi analize, to može biti svakodnevno, a može biti svakih nekoliko mjeseci. Tako na primjer, velike tvrtke s visokim stupnjem redundantnosti u poslovanju mogu plan provjeravati na svakodnevnoj osnovi. Možda najučinkovitija metoda, ali ujedno i najjednostavnija za provedbu vježbe je namjerno prekidanje poslovanja nekog odjela tvrtke te prebacivanje tog dijela posla na ostale odjele, u skladu sa smjernicama u planu za ponovnu uspostavu poslovnih procesa. Tako ne samo da provjeravaju učinkovitost donesenog plana nego i vježbaju zaposlenike za njegovu bržu primjenu. Samim time podižu svijest o važnosti upravljanja kontinuitetom poslovnih procesa, ali i znanje zaposlenika o tim procesima unutar tvrtke.

Provedbom plana provjerava se zadovoljava li on sve ključne potrebe poslovanja odnosno da li je ponovna uspostava nekog ključnog poslovnog procesa previđena. Također, dolazi na vidjelo je li plan uopće provediv odnosno je li neke korake u ponovnoj uspostavi poslovnih procesa potrebno zamijeniti ili doraditi.

Postoje tri kategorije provjere plana, prema složenosti i obuhvatnosti provjere:

- jednostavna provjera,
- srednje složena provjera i
- složena provjera.

Ove provjere detaljnije su opisane u narednim poglavljima.

4.1. Jednostavna provjera

Jednostavna provjera sastoji se od provjere specifičnog vida plana za ponovno uspostavljanje poslovnih procesa. To mogu biti ljudski resursi ili, na primjer, provjera informatičke opreme. Takva provjera u pravilu uključuje najviše 20 djelatnika i ne bi trebala trajati duže od tri sata.

Na jednostavnim provjerama, u pravilu, sudjeluju djelatnici odgovorni za primjenu plana u određenom području poslovanja tvrtke.

4.2. Srednje složena provjera

Prilikom ove vrste provjere dolazi do potrebe za suradnjom među različitim odjelima tvrtke, odnosno njihovim odgovornim timovima. Ovdje se prelazi s osnovne rasprave o mogućim prijetnjama, na pokušaj stvarnog rješavanja neke od njih. Naglasak se stavlja na vjerodostojnost vježbe i vremenski pritisak koji takva prijetnja uzrokuje. Ovakve vježbe mogu trajati i po nekoliko dana.

4.3. Složena provjera

Kao najsveobuhvatnija provjera plana, i vid uvježbavanja djelatnika, složena provjera može se provoditi bez najave te može obuhvatiti cijelu tvrtku. Ona u biti predstavlja stvaran pokušaj rješavanja neke prijetnje. Na primjer, stvarno seljenje poslovanja na drugo mjesto odnosno adresu. Prilikom ovakve provjere dolazi se do vrijednih podataka za sam plan i njegove buduće inačice. Može se uspostaviti da je za već spomenuto seljenje potrebno znatno više vremena nego je planom za to predviđeno. Tada se provjerava prihvatljivost novih rezultata te, ako je potrebno, traži novo rješenje.

Ovakve provjere plana ne služe samo za njegovo poboljšanje ili za uvježbavanje djelatnika bržem uspostavljanju poslovnih procesa u slučaju nezgode. One doprinose njegovom prihvaćanju među djelatnicima, te kao način za podizanje svijesti zaposlenika o stvarnim rizicima za poslovanje i tvrtku, a samim time i njih same ili barem njihov posao. Samo prihvaćanje plana među djelatnicima ključno je za njegovu uspješnu provedbu u slučaju nezgode.

Slika 3. *Dijelovi upravljanja kontinuitetom poslovnih procesa*
Izvor: *Bussines Continuity Institute*

5. Prilagodba plana promjenama

Održavanje relevantnosti samog plana sastoji se od tri dijela. Sve provjere i promjene plana odvijaju se periodično, a dijelimo ih na:

1. Provjera i promjena podataka o samoj tvrtki, ustroju i djelatnicima, distribucija promijenjene inačice plana odgovornim djelatnicima, odnosno timu za upravljanje.
2. Provjera tehničkih rješenja za određene prijetnje, navedenih u samom planu.
3. Provjera procesa za ponovno uspostavljanje poslovanja.

5.1. Provjera i promjena podataka

Sve se organizacije mijenjaju s vremenom, pa se tako i plan za upravljanje poslovnim procesima, ali i priručnik za ponovno uspostavljanje poslovnih procesa treba mijenjati u skladu s tvrtkom. U protivnom će tvrtka imati plan koji joj uopće ne odgovara. Najčešći podaci koje treba redovito mijenjati u svakom ciklusu plana (slika 1.) za upravljanje kontinuitetom poslovnih procesa su:

- promjene zaposlenika i njihovog broja, te samim time i promjene tima za upravljanje i donošenje odluka,
- promjene u samoj strukturi tvrtke,
- promjene važnih klijenata i/ili njihovih podataka za kontakt,
- promjene ključnih dobavljača i/ili njihovih podataka za kontakt,
- promjene u samoj djelatnosti tvrtke.

Redovitost tih ciklusa ovisi o dinamičnosti poslovanja tvrtke.

5.2. Provjera odgovora na pojedine prijetnje

Kako tehnologija napreduje, a i sami djelatni procesi se mijenjaju, mijenja se i odgovarajuća metoda kako odgovoriti na pojedine prijetnje. Da bi odgovori bili najučinkovitiji, potrebno je u svakom ciklusu upravljanja kontinuitetom poslovnih procesa primijeniti metodu prilagođenu vremenu u kojem se upravljanje provodi. Najčešće provjere odgovora na neke uobičajene prijetnje mogle bi biti:

- obrana i oporavak od napada zlonamjernim računalnim programima,
- provjera same računalne sigurnosti tvrtke te
- provjera same fizičke opreme te njene ispravnosti.

5.3. Provjera procesa za ponovno uspostavljanje poslovanja

Prilikom provođenja plana i provjere procesa za ponovno uspostavljanje poslovanja (4. Provođenje plana) provjerava se i po potrebi mijenja procedura za odgovor na prijetnje iz poglavlja (5.2. Provjera odgovora na pojedine prijetnje) u slučaju da su iste ipak uspjele zaustaviti odnosno prekinuti poslovanje tvrtke. Također, jedna od ključnih provjera jest jesu li svi poslovni procesi cjelokupno dokumentirani te jesu li smjernice za njihovo ponovno pokretanje dovoljno razumljive odnosno „čitljive“ timu za upravljanje i donošenje odluka.

U skladu s uočenim problemima prilikom provođenja i provjere plana, on se može mijenjati. To rezultira novom inačicom plana i priručnika za ponovno uspostavljanje poslovanja prilikom svakog ciklusa (slika 1) upravljanja kontinuitetom poslovanja. Tako se ciklus upravljanja kontinuitetom poslovanja zatvara, odnosno počinje novi, te se plan stalno unaprjeđuje.

6. Upravljanje kontinuitetom poslovnih procesa u Hrvatskoj i u svijetu

6.1. U svijetu

Upravljanje kontinuitetom poslovnih procesa te planiranje u slučaju potrebe za ponovnom uspostavom poslovnih procesa je uobičajena stvar u svijetu. Primjeri takvih planova se čak mogu preuzeti sa Internet poslužitelja stranih vlada. Jedan takav plan nalazi se na Internet stranicama vlade Sjedinjenih Američkih Država:

http://www.ready.gov/america/_downloads/sampleplan.pdf

U razvijenijim zemljama kao što su Sjedinjene Američke Države, Japan ili Velika Britanija, neki dijelovi upravljanja kontinuitetom poslovnih procesa su propisani zakonom paih se svaka tvrtka ili organizacija dužna pridržavati.

Nakon terorističkog napada na Sjedinjene Američke države, 11. rujna 2001. godine, mnoge tvrtke u Americi čuvaju čak i veće zalihe hrane u sklopu poslovnog prostora u slučaju nezgode koja može zarobiti djelatnike u poslovnom prostoru. Usprkos cijeni i vremenu potrebnom za upravljanje kontinuitetom poslovnih procesa sve više i više tvrtki donosi planove za uspostavu i održavanje poslovnih procesa u slučaju nezgode.

6.2. U Hrvatskoj

Kako i u mnogočemu, Republika Hrvatska još nije na razini zapadnih zemalja u učestalosti planiranja kontinuiteta poslovanja među tvrtkama. Međutim napredak kroz godine je vidljiv. Sve više tvrtki upravlja kontinuitetom svojih poslovnih procesa, ali i sve više tvrtki nudi usluge upravljanja kontinuitetom poslovnih procesa. Većinom se to odnosi na upravljanje i održavanje informatičke i telekomunikacijske infrastrukture te upravljanje sigurnosnim kopijama podataka. Ali za najveći broj malih i srednjih tvrtki to je dovoljno i jedino ključno za kontinuitet poslovanja.

7. Zaključak

S porastom veličine tvrtke, te obujma njenog poslovanja, raste i složenost upravljanja kontinuitetom poslovnih procesa. Sam plan za ponovnu uspostavu poslovanja i poslovnih procesa nužan je, u nekom obliku, za svaku tvrtku, barem za najčešće oblike rizika poslovanju. U malim tvrtkama s nekoliko zaposlenika, nedostatak fizičkog priručnika u slučaju „katastrofe“ možda nije ni nužan jer koordinacija i komunikacija među djelatnicima nije toliko zahtjevna. Takvim tvrtkama je dovoljna jedna osoba za održavanje ključnih podataka o poslovanju, kao što je popis klijenata i dobavljača. Svejedno, kao osnovni korak upravljanja kontinuitetom poslovnih procesa je izrada sigurnosnih kopija ključnih podataka, po mogućnosti na udaljenom mjestu. Međutim, kod većih organizacija provedba plana za upravljanje kontinuitetom poslovnih procesa je značajno složenija i zahtjeva unajmljivanje profesionalaca za njegovu provedbu i temeljite provjere.

Na svu sreću i na području Republike Hrvatske posluju organizacije sposobne kvalitetno provesti takve planove.

Koliko je često potrebno provoditi reviziju plana kontinuiteta poslovnih procesa ovisi o tome koliko su česte organizacijske promjene. Dobro je pravilo da neovisno o promjenama, tim zadužen za upravljanje kontinuitetom poslovnih procesa provodi provjere barem dva puta godišnje. Ovisno o prirodi promjena unutar tvrtke, tim će prilikom svake promjene imati veću ili manju količinu podataka za izmijeniti odnosno prilagoditi trenutnom stanju u tvrtki. Prema količini potrebnih izmjena u svakom ciklusu (slika 1.) može se planirati povećanje učestalosti revizije plana ili njeno smanjenje.

Leksikon pojmova

Upravljanje kontinuitetom poslovnih procesa (eng. Business continuity planning, BCP ili Business continuity management, BCM)

Proces izrade i dorade logističkog plana koji daje smjernice kako izbjeći, ublažiti, te u slučaju najgoreg, oporaviti se, odnosno ponovno pokrenuti poslovanje, nakon kraha uzrokovanog nezgodom.

http://en.wikipedia.org/wiki/Business_continuity_planning

RPO (eng. Recovery Point Objective)

Prihvatljiva količina gubitka poslovnih podataka, odnosno najstarije dopušteno vrijeme iz kojeg je potrebno povratiti poslovne podatke.

http://en.wikipedia.org/wiki/Recovery_point_objective

RTO (eng. Recovery Time Objective)

Prihvatljiva količina vremena potrebnog za ponovno pokretanje određenog poslovnog i/ili organizacijskog procesa odnosno prikupljanje količine podataka navedenih u RPO.

http://en.wikipedia.org/wiki/Recovery_time_objective

MTDL (eng. Maximum Tolerable Data Loss)

Najveći dozvoljen gubitak podataka.

MTPD (eng. Maximum Tolerable Period of Disruption)

Vremenski period dozvoljen za ponovno uspostavljanje određenog procesa.

8. Reference

[1] Wikipedia, Business continuuity planning, http://en.wikipedia.org/wiki/Business_continuity_planning, lipanj 2011. godine,

[2] Wikihow, Craete a Business Continuity Plan, http://www.wikihow.com/Create-a-Business-Continuity-Plan, lipanj 2011. godine,

[3] Business Continuity and Disaster Recovery Planning: The Basics, http://www.csoonline.com/article/204450/business-continuity-and-disaster-recovery-planning-the-basics, lipanj 2011. godine,

[4] Business Continuity Planning/Disaster Recovery Planning, http://www.yourwindow.to/business-continuity/, srpanj 2011. godine,

[5] John Williamson, „Business Continuity Planning: A Primer for Management and IT Personnel“, http://www.allhandsconsulting.com/toolbox/BCP_2-07a.PDF, srpanj 2002. godine,

[6] Business Continuity Institute, http://www.thebci.org/, srpanj 2011. godine.