



U pitanju nisu samo ekonomski interesi, nego šira društvena odgovornost tvrtke prema korisnicima, vlasnicima, zaposlenicima i društvu u cjelini. Prihvaćanje te odgovornosti znači spremnost za savjesno, društveno odgovorno poslovanje

Zašto uopće upravljati kontinuitetom poslovanja?

Porast primjene e-trgovanja i uporabe Interneta u poslovne svrhe stvorili su potrebu za kontinuiranim pružanjem usluga korisnicima. Zahtjevi za raspoloživošću poslovnih sustava 24x365 i prosječno vrijeme otklona greške između 2 i 24 sata postali su standard, uvjetovan očekivanjima svih zainteresiranih strana:

- Korisnici očekuju stalnu raspoloživost usluge,
- Investitori očekuju povećanje vrijednosti ulaganja neovisno o okolnostima,
- Vlasnici očekuju da će upravljanje tvrtkom operativno funkcionirati u svim situacijama,
- Zaposlenici očekuju da će njihova egzistencija biti osigurana,
- Opskrbljivači očekuju da će njihova zarada nastaviti pristizati,
- Regulatorna tijela očekuju da će njihovi zahtjevi biti ispoštovani neovisno o okolnostima,

Održavanje kontinuiteta poslovanja je u tom smislu kritičan i izuzetno zahtjevan zadatak. Upravljanje kontinuitetom poslovanja, kvalitetno podržano na svim razinama, utjelovljuje strateški okvir za izbjegavanje rizika koji mogu uzrokovati:

- Ispad poslovnog procesa,
- Ispad korisničke usluge,
- Gubitak imovine,
- Zakonsku odgovornost,
- Štetu ugledu tvrtke.

U pitanju nisu samo ekonomski interesi, nego šira društvena odgovornost tvrtke prema korisnicima, vlasnicima, zaposlenicima i društvu u cjelini. Prihvaćanje te odgovornosti znači spremnost za savjesno, društveno odgovorno poslovanje. Glavni izazov nije tehnologija, već stvaranje svijesti o potrebi društveno odgovornog pristupa na svim organizacijskim razinama i njegovo ugrađivanje u temelje

korporativne kulture. Na tržištu postoji čitav niz rješenja i usluga koje ciljaju neki od elemenata održavanja kontinuiteta poslovanja (izrada BCP-a i DRP-a, sigurnost, podatkovni centri, virtualizacija), no RECRO-NET ovoj problematici pristupa kroz ukupnost rješenja posebno prilagođenog svakom korisniku. RECRO-NET u tom smislu upravljanje kontinuitetom poslovanja ne sagledava samo kao poslovno-tehnološku disciplinu, nego kao stratešku odrednicu razvoja svake tvrtke.

Kako održati kontinuitet poslovanja?

Održavanje kontinuiteta poslovanja nekog poslovnog subjekta obuhvaća i poslovno i tehnološki širi kontekst od medijski najčešće ciljanog procesa Upravljanja kontinuitetom poslovanja (Business Continuity Management - BCM). BCM je definiran u ISO/IEC 27002 Section 10 kao kontinuirani proces u okviru kojeg se razmatraju potencijalni rizici za poslovanje i osigurava neprekinutost ključnih poslovnih procesa u slučaju nastanka štetnog događaja. Štetnim se događajem smatraju sve pojave koje narušavaju normalno poslovanje: prirodne katastrofe, eksplozije, požari, kemijski, biološki i nuklearni incidenti, ispadi električnog napajanja, HW/SW greške, oštećivanje podataka.

BCM kao takav razmatra obuhvaća i definira aktivnosti:

- predviđanja mogućih štetnih događaja i njihovog utjecaja na poslovanje,
- izrade plana postupaka i procedura u slučaju nastanka takvih događaja,
- implementacije postupaka i mehanizama reakcije u trenutku nastanka,
- periodičke provjere funkcioniranja implementiranih mehanizama.

Praktično primjenjivi rezultat BCM procesa je Plan održavanja kontinuiteta poslovanja

(Business Continuity Plan - BCP) i kao takav uključuje planiranje za non-ICT segmente kao što su ljudski resursi, prostori i objekti, komunikacija i zaštita kredibiliteta, a oslanja se na Plan tehnološkog oporavka (Disaster Recovery Plan - DRP) za ICT segmente. Plan tehnološkog oporavka definira organizaciju, postupke, procedure i tehnološku infrastrukturu koji će osigurati nastavak normalnog funkcioniranja ICT infrastrukture (aplikacije, mreža, oprema, podaci) kritične za poslovanje nakon nastupanja štetnog događaja. U tom smislu BCM proces obuhvaća definiranje reakcija na svim razinama u slučaju nastanka štetnog događaja.

No prevencija, odnosno smanjivanje uopće mogućnosti nastajanja štetnih događaja, ključna je aktivnost koja se mora provoditi u svim segmentima poslovanja. Kako je informacijsko-komunikacijska infrastruktura podloga za implementaciju poslovnih sustava i procesa te podršku istima, kontinuitet se poslovanja osigurava već u sferi informacijsko-komunikacijske tehnologije i nužno ga je promatrati kroz tri temeljna elementa:

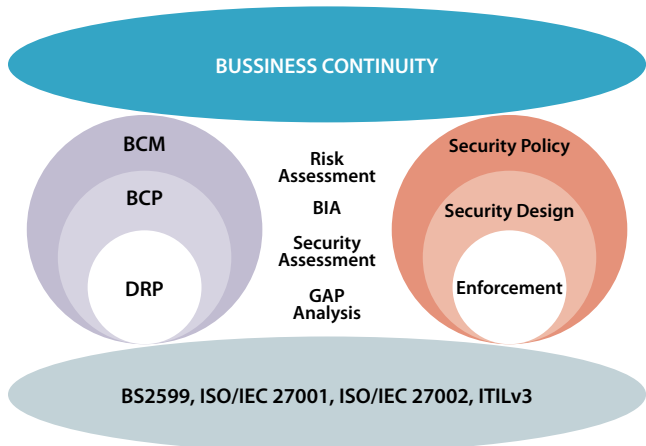
- sigurnost ICT sustava,
- zalihost ICT sustava,
- standardizacija.

Zajedničko je polazište BCM procesa i sigurnosti ICT sustava kvalitetno predviđanje i planiranje koje se provodi kroz sljedeće aktivnosti:

- procjena mogućih sigurnosnih incidenata i vrijednosti resursa (Risk Assessment),
 - procjena utjecaja sigurnosnog incidenta na poslovanje (Business Impact Analysis - BIA)
- Ove aktivnosti trebaju osigurati ključne ulazne podatke za definiranje dvaju relacijski povezanih segmenata - Sigurnosne politike (ISO/IEC 27002 Section 1) i prethodno opisanog Plana održavanja kontinuiteta poslovanja kao

produkta procesa Upravljanja kontinuitetom poslovanja.

Paradigma sigurnosti seže značajno izvan okvira informacijsko-komunikacijske tehnologije, no ako se sigurnosni aspekt promatra isključivo kroz tehnološku perspektivu, ona se načelno svodi na dvije razine: fizičku sigurnost (ISO/IEC 27002 Section 5) i sigurnost komunikacija i operacija (ISO/IEC 27002 Section 6), čija je krajnja svrha očuvanje povjerljivosti, integriteta i dostupnosti podataka, odnosno zaštita informacija. Kroz zadovoljavanje sigurnosnih pretpostavki navedenih razina ispunjava se jedan od preduvjeta održavanja kontinuiteta poslovanja. Sustavni pristup definiranju i održavanju sigurnosnog okruženja podrazumijeva kontinuirani proces s vrlo preciznim ciklusom trajanja koji obuhvaća planiranje, dizajn, implementaciju, praćenje i prilagodbu sigurnosnog sustava. Razborita procjena mogućih sigurnosnih incidenata, definiranje optimalnih metoda, alata i aktivnosti zaštite, striktna primjena metoda i provođenje definiranih aktivnosti te standardizacija procesa mogu rizik od sigurnosnog incidenta svesti na mjeru koju



• **Temeljni elementi** upravljanja kontinuitetom poslovanja

je moguće kontrolirati. Temeljne su aktivnosti u tom smislu:

- kreiranje koncepta sigurnosne politike (Security Policy),
- definiranje sigurnosnih metoda i alata (Security Design).

Sigurnosna politika načelno definira opći stav poslovnog subjekta prema informacijskoj sigurnosti, poslovno temeljene zahtjeve informacijske sigurnosti te opseg i zadatke Sustava upravljanja informacijskom sigurnosti (Information Security Management System - ISMS). Ključno je uskladiti značaj/vrijednost štićenih resursa i vrijednost sigurnosnog sustava, odnosno postići prihvatljivi kompromis između potreba i mogućnosti, uvjetovanih financijskim, organizacijskim i tehničkim ograničenjima.

Budući da je najčešća situacija u praksi takva da korisnici već imaju implementirane određene sigurnosne sustave, sastavni je dio procesa planiranja i procjena postojećeg sigurnosnog sustava (Security Assessment). Ona obuhvaća pregled sigurnosne politike i dizajna, pregled implementiranih mehaniza-

ma te utvrđivanje raskoraka (GAP Analysis), poredbenom analizom prikupljenih podataka. Po potrebi se može pristupiti i testiranju sigurnosti sustava kroz penetracijske testove. Temeljem rezultata analize, i eventualnog testa, preciznije se određuju slabe točke sustava i na taj način dobivaju kvalitetniji ulazni podaci nužni u prethodno opisanim fazama planiranja i dizajniranja.

Kakvoća provedbe navedenih aktivnosti planiranja i dizajniranja izravno će utjecati na operativnost sigurnosnog sustava te posljedično njegovu učinkovitost i svrsishodnost u cjelini. Kao i uvijek, poanta je naći pravu mjeru na način da sustav zaštite ne oteža ili onemogućiti normalno funkcioniranje poslovnog sustava.

Drugi je element bitan za održavanje kontinuiteta poslovanja zalihost informacijsko-komunikacijskog sustava u smislu redundancije objekata, veza, uređaja i samih podataka. Podatkovni se centar najčešće promatra kao središnja točka svakog informacijsko-komunikacijskog sustava. Stoga su temeljni zahtjevi koji se postavljaju na podatkovni centar pouzdanost i visoka raspoloživost (High Availability).

Tehnologija se podatkovnih centara značajno razvila i standardizirala posljednjih godina, a tehnološki je napredak posebice vidljiv na području virtualizacije ICT resursa (serveri, storage, mreža). Prednosti i uštede koje donosi virtualizacija takve su da je koncept u kratko vrijeme postao već uvriježeni standard kod svih važnijih proizvođača. Relevantna globalna regulativa (HIPAA, Basel II, EFA, GASB, COOP, COG) zahtijeva/preporučuje definiranje BCP-a i DRP-

te neizravno upućuje na potrebu izgradnje dislociranih podatkovnih centara (Disaster Recovery Center - DRC) kao obveznu poslovnu praksu. Konačno, standardizacija kao treći element bitan za održavanje kontinuiteta poslovanja podrazumijeva realno primjenjivo pridržavanje regulatornih i tehnoloških preporuka te nužno prožima prethodno opisane elemente sigurnosti i zalihosti ICT sustava. Relevantni međunarodni standardi BS25999, ISO/IEC 27001, ISO/IEC 27002 zahtijevaju donošenje jasne Sigurnosne i BC politike na kojima će se temeljiti operativno planiranje i provedba. ISO/IEC 27002 najaktualniji je globalni sigurnosni standard koji, između ostalog, u svom Section 10 zahtijeva izradu odgovarajućih Planova održavanja kontinuiteta poslovanja (BCP) i tehnološkog oporavka (DRP). ISO/IEC 27002 Section 11 obrađuje pitanje regulatorne usklađenosti (Compliance) s relevantnim nacionalnim i globalnim zakonima te profesionalnim standardima.

Kako to izgleda u praksi?

Navedeni standardi i preporuke u teorijskom smislu pokrivaju sve ICT aspekte nužne za

održavanje kontinuiteta poslovanja. No, praktična primjena i poštivanje tih preporuka odgovornost su svakog poslovnog subjekta i kao takvi izravno ukazuju na razinu korporativne kulture i svijesti. Čitav je niz objektivnih i subjektivnih poteškoća s kojima se neizbježno susreće većina pokušaja ozbiljnijeg pristupa ovoj problematici. Visoko kompetitivna tržišta, posebice ona u razvoju, stavljaju uprave i operativna rukovodstva tvrtki u poziciju u kojoj su opterećeni prvenstveno egzistencijalnim pitanjima pa se teško nalazi prostora i vremena, a još manje financijskih mogućnosti za sustavniju primjenu ovakvog koncepta. Ne treba sumnjati da svijest o potrebi održavanja kontinuiteta poslovanja kod većine tvrtki postoji, ali su pritisci svakodnevnih operativnih naprezanja jednostavno preveliki.

S druge strane, postupci uvođenja ovakve prakse u poslovanje su nerijetko toliko birokratizirani i daleko od prakse da profesionalci zaziru od susreta s 'iskusnim stručnjacima' i all-in-wonder tablicama koje sadrže frustrirajuće setove pitanja. Isto tako još uvijek ima i onih za koje uvođenje upravljanja kontinuitetom poslovanja predstavlja samo regulatorni alibi i takvo trošenje dragocjenih materijalnih i ljudskih resursa neće dati očekivane učinke. Ulazak u EU jednostavno će otkloniti svaku alternativu sustavnoj primjeni standardiziranog upravljanja kontinuitetom poslovanja. Koliko god su trenutno regulatorni zahtjevi glavni pokretač razmišljanja o uvođenju BCM koncepta u praksu, toliko će samo tržište i korisnici postupno eliminirati one koji ne počnu funkcionirati po modelu društveno odgovornog poslovanja. •

RECRO-NET i partneri

RECRO-NET je, uz podršku svojih tehnoloških partnera, već spreman za takve tržišne uvjete i kontinuirano razvijati ekspertizu nužnu za kvalitetno pokrivanje svih segmenata koji čine širu perspektivu upravljanja kontinuitetom poslovanja. Iskustva s već realiziranih projekata u Hrvatskoj, regiji i Bliskom istoku omogućuju nam stalno usavršavanje koncepta. S obzirom na širinu znanja i vještina potrebnih za kvalitetno vođenje korisnika kroz proces izgrađivanja vlastitog sustava upravljanja kontinuitetom poslovanja, nekoliko tehničkih odjela RECRO-NETA pokriva segmente sigurnosti, podatkovnih centara te pripreme BCP-a i DRP-a. RECRO-NETOVA metodologija definira standardizirani okvir, ali se sadržaj i tijek procesa prilagođavaju realnom poslovnim okruženju pojedinog korisnika. Metodologija se zasniva na višegodišnjem praktičnom iskustvu u ICT industriji zahvaljujući kojem RECRO-NET kreira i podržava cjelokupni proces i primjenu standarda, učinkovito ih prilagođavajući stvarnim poslovnim potrebama korisnika.