Vrsta rada: Originalni naučni rad
Primljen: 27. 4. 2022.
Prihvaćen: 1. 6. 2022.
UDK:

Plan oporavka od katastrofe u slučaju prekida poslovanja i gubitka podataka

Goran Bogosavljević[1]
[1]Visoka škola strukovnih studija za informacione tehnologije – ITS, master strukovne studije,Beograd, Srbija
Kontakt informacije: goran46521@its.edu.rs

Sažetak – Danas se podaci generišu u velikim količinama. Znamo da računarstvo u oblaku predstavlja novu vrstu računarske platforme u današnjem svetu. Ova vrsta računarstva generiše veliku količinu privatnih podataka u oblaku. Stoga potreba za uslugama koje se tiču oporavka podataka raste iz dana u dan i zahteva razvoj efikasne i efektivne tehnike oporavka podataka. Svrha ovog rada je da predoči tehnike oporavka i pomogne korisniku da prikupi informacije sa bilo kog rezervnog servera kada je server izgubio svoje podatke i nije u mogućnosti da pruži povratne informacije korisniku. Takođe, biće reči o nekoliko tehnika oporavka podataka u oblaku s ciljem zaštite podataka i kontinuiteta poslovanja u slučaju neplaniranog prekida ili katastrofe, bilo prirodne ili izazvane ljudskom greškom ili namerom.

Ključne reči: (RTO), (RPO), (DRP), (CC), (DR)

I. UVOD

Računarstvo u oblaku je računarski proces zasnovan na internetu, u kome su sistemi međusobno povezani sa međusobnim deljenjem resursa. Internet je medij između oblaka i korisnika. Klijent je povezan sa serverom u oblaku i može da skladišti podatke putem interneta i može da pristupi podacima sa bilo kog mesta. To je komunikaciona mreža u realnom vremenu, gde je moguće pokrenuti naše programe sa bilo kog mesta pristupom oblaku. Kada dođe do pada sistema ili nestanka struje, postoji mogućnost gubitka podataka, a ponekad to može dovesti do finansijskog gubitka. Rušenje ovog sistema i drugi problemi nastaju usled prirodnih katastrofa ili zbog ljudskog faktora.

Kada dođe do katastrofe, kompanija treba da zaštiti podatke od gubitka. Kompanije koje pružaju usluge u oblaku su Google, Amazon, Microsoft itd. Kada dođe do katastrofe na strani klijenta, rezervna kopija će biti uskladištena u oblaku, ali ako dođe do katastrofe u oblaku, podaci će biti izgubljeni.

Da bi se ove katastrofe prevazišle, postoje neke tehnike oporavka od katastrofe koje se koriste za oporavak podataka i koje su potrebne za kontinuitet poslovanja. Svaka organizacija treba da ima dokumentovan proces oporavka od katastrofe i treba da testira taj proces najmanje dva puta godišnje.

II. UZROCI GUBITKA PODATAKA

The Disaster Recovery Institute International (www.drii.org) piše da se 93% kompanija koje su iskusile neku vrstu katastrofe, a nisu imale plan oporavka, zatvorilo u roku od pet godina. Takođe, 50% kompanija koje dožive prekide kritičnih poslovnih funkcija duže od deset dana nikada se potpuno ne oporave. Ovo je posebno zanimljiv podatak za kompanije koje pripadaju listi kompanija „Fortune 500", jer ih zastoji u poslovnim operacijama u proseku koštaju 96.000 dolara po minuti.

A. Prirodne katastrofe

Kada dođe do prirodnih katastrofa, tada će biti izgubljena velika količina podataka, ukoliko ne postoji pripremljen Disaster Recovery Plan (DRP). Pojava i jačina pojedinih prirodnih katastrofa, poput oluja, snega, uragana ili pak jakih kiša, mogu se predvideti i približno proceniti. Neke opasnosti kao što su potresi, požari, vulkanske erupcije i klizišta imaju nepredvidivu narav i time predstavljaju potencijalno mnogo veću pretnju. [1]

B. Katastrofe uzrokovane ljudskim faktorom

Pored prirodnih katastrofa, veliki deo čine katastrofe uzrokovane ljudskim nemarom i greškama. Većina katastrofa uzrokovana na ovaj način namerno je izazvana, dok se samo pojedine mogu svrstati pod slučajnost. Kako ih nije lako kategorisati, nabrojaću neke: terorizam, bombardovanje, sajbernapadi, krađe, oružani napadi, biološki napadi.

C. Nesreće i tehnološke katastrofe

Mogu biti izazvane ljudskim ali i spoljnim faktorom. Kod ljudskog je razlika u odnosu na prošle u nameri. Nisu namerno uzrokovane, već su posledica nepažljivog održavanja. U spoljne faktore na koje se ne može uticati spadaju: nesreće povezane sa prekidom napajanja ili električnom energijom, urušavanje građevinskih objekata, pad i nedostupnost informacijske i komunikacijske infrastrukture.

D. Upad u mrežu

Kada virus napadne aplikacije, postoji šansa da dođe do katastrofe.

E. Hakovanje ili zlonamerni kod

Katastrofa se dešava unutar ili van organizacije. Iako one ulažu dosta napora da spreče hakovanje ili da zlonamerni kod modifikuje podatke, dolazi do gubitka podataka.

III. TRADICIONALNI OPORAVAK OD KATASTROFE

Tradicionalni oporavak od katastrofe je tokom svog razvoja podeljen u nekoliko nivoa. [2]

F. Nivo 0

Nema podataka van lokacije, što znači da nema plana oporavka od katastrofe niti sačuvanih podataka. Oporavak podataka može potrajati nedeljama i neće biti uspešan.

G. Nivo 1

Rezervna kopija podataka bez hotsitea, što znači da se rezervna kopija podataka preuzima van lokacije, a ne putem hotsitea. Preuzimanje podataka za koje je napravljena rezervna kopija je proces koji traje dugo. Pošto kompanija nema sopstvene redundantne servere, potrebno je vreme da se locira i konfiguriše odgovarajući sistem.

H. Nivo 2

Backup podataka sa hotsiteom, što znači da organizacije održavaju rezervnu kopiju podataka, kao i hotsite, i to je najbrži proces. Ukoliko postoji vruća rezervna lokacija kada dođe do katastrofe, mogu se pokrenuti aplikacije na serverima u pripravnosti.

IV. ZAHTEVI ZA OPORAVAK OD KATASTROFE

Prilikom oporavka od katastrofe definišu se zahtevi i objašnjavamo dve ključne karakteristike za efikasnu uslugu u oblaku kada dođe do katastrofe.

I. Ciljna tačka oporavka

Maksimalni period potreban za gubitak podataka, kada dođe do katastrofe (Recovery Point Objective – (RPO), ciljna tačka oporavka) . Neophodan RPO je generalno poslovna odluka – za neke aplikacije apsolutno nijedan podatak ne sme da se izgubi (RPO = 0), što zahteva da se koristi kontinuirana sinhrona replikacija, dok za druge aplikacije prihvatljiv gubitak podataka može da se kreće od nekoliko sekundi do nekoliko sati ili čak dana. Ciljna tačka oporavka identifikuje koliko podataka je kompanija spremna da izgubi u slučaju katastrofe. RPO je obično vođen načinom na koji se čuvaju i prave rezervne kopije podataka [1]:

» Nedeljne rezervne kopije van lokacije će preživeti gubitak centra podataka, dok će izgubiti količinu nedeljnih podataka. Pravljenje dnevnih rezervnih kopija van lokacije je još bolje.
» Svakodnevne rezervne kopije na licu mesta će preživeti gubitak datog proizvodnog okruženja sa danom gubitka podataka plus repliciranjem transakcija tokom perioda oporavka nakon gubitka sistema. Pravljenje rezervnih kopija na licu mesta po satu je još bolje.
» Grupisana baza podataka u više centara podataka će preživeti gubitak svakog pojedinačnog centra podataka bez gubitka podataka.

J. Ciljno vreme oporavka

Ciljno vreme oporavka (RTO) predstavlja merenje vremena do oporavka poslovnih procesa kada dođe do katastrofe i prekida rada. To mogu biti minuti, sati i dani. Takođe, može uključivati otkrivanje kvara i pripremu potrebnih servera na lokaciji rezervne kopije za inicijalizaciju aplikacije koja je prekinuta usred izvršenja. Ciljno vreme oporavka identifikuje koliko je zastoja prihvatljivo u slučaju katastrofe.

V. PLAN OPORAVKA OD KATASTROFE

Postoje neki mehanizmi koji se primenjuju za pravljenje rezervnih kopija podataka kada se koristi tehnika oporavka od katastrofe. U literaturi se uglavnom navode tri modela za implementaciju mirroringa ili preslikavanja sajta, i to: vrući (hot), topli (warm) i hladni (cold) backup sajta. Lokacije za rezervne kopije mogu doći iz tri različita izvora [5]:

» kompanije specijalizovane za pružanje usluga oporavka od katastrofe;
» druge lokacije u vlasništvu i lokacije kojima upravlja organizacija;
» zajednički dogovor sa drugom organizacijom da deli objekte centra podataka u slučaju katastrofe.

K. Hot Backup Site

Veoma je skup za rad. Ovaj sajt radi sa organizacijama koje upravljaju procesima u realnom vremenu.

To je duplikat originalnog sajta. Gubitak podataka je minimalan, jer se podaci mogu premestiti i nastaviti nesmetan rad. Za nekoliko sati lokacija Hot Backup Site može dovesti do pune proizvodnje.

L. Cold Backup Site

Najjeftiniji je za rad. Ne zahteva nikakve rezervne kopije podataka ili ne uključuje hardver. Usled nedostataka hardvera može započeti sa minimalnim troškovima, ali zahteva više vremena za oporavak u slučaju katastrofe . Sve što je potrebno za vraćanje usluge korisnicima mora biti nabavljeno i isporučeno na lokaciju pre nego što se izvrši operacija oporavka.

M. Warm Backup Site

Već je opremljen hardverskom konfiguracijom na lokaciji rezervne kopije koja se nalazi na primarnoj lokaciji. Da bi se primenio Warm Backup Site, poslednja rezervna kopija podataka treba da bude isporučena na njihove primarne lokacije.

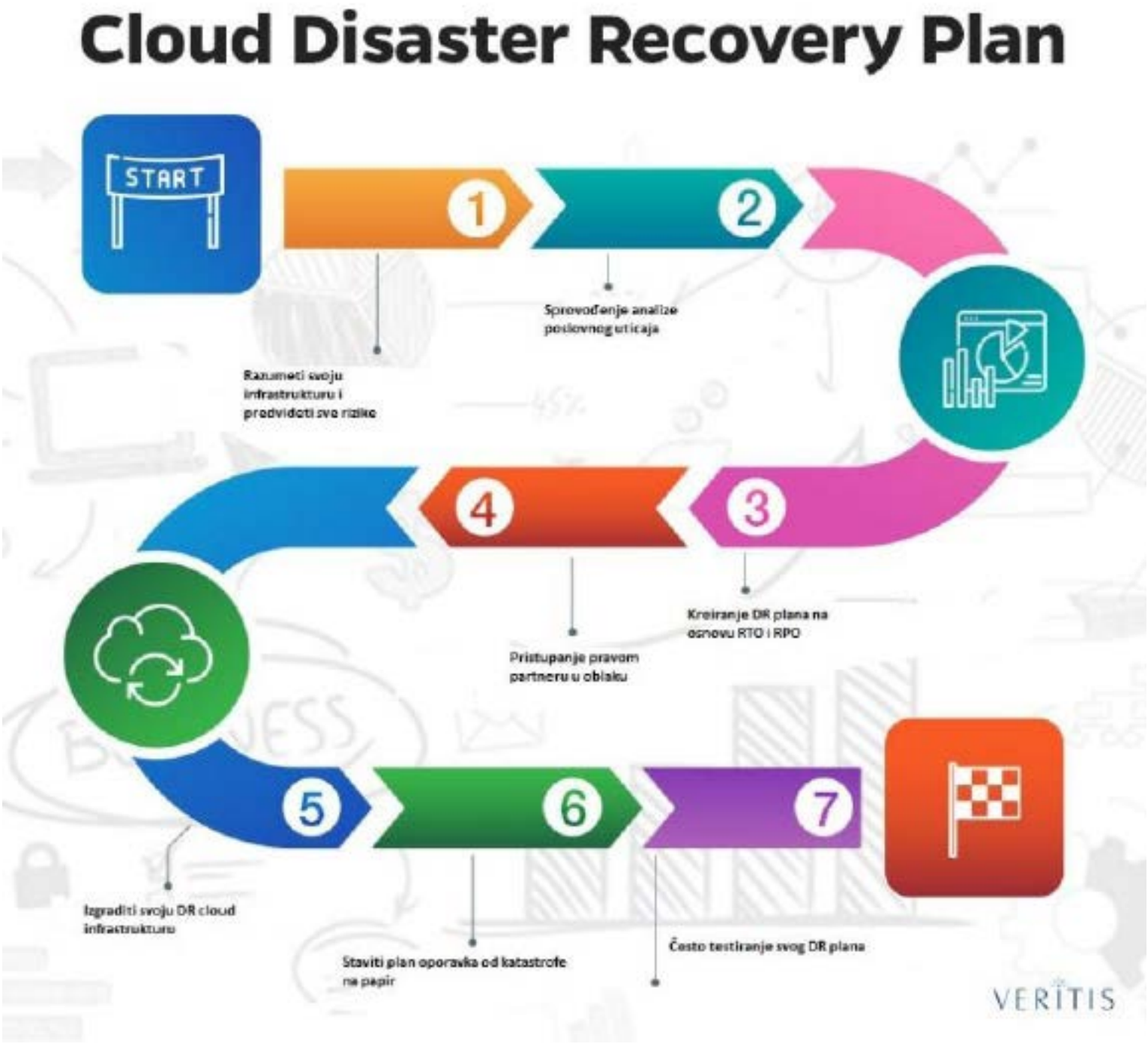
U svetu u kome tehnologija pokreće skoro svaki aspekt naših života, oblak je zaista unapredio ovo iskustvo. Od preuzimanja složenih operativnih opterećenja do izvođenja velikih planova oporavka od katastrofe, oblak je učinio naše svakodnevne operacije gotovo lakim.

Dolaženjem do složenog zadatka kao što je upravljanje operacijom oporavka od katastrofe oblak nas je naterao da razmislimo koliko je bilo teško sprovesti projekat oporavka od katastrofe pre njegovog dolaska.

Ako bi katastrofa pogodila primarni centar podataka, morali biste da obezbedite rezervni centar podataka, koji, naravno, dolazi sa dvostrukim radom, uključujući [3]:

- postavljanje fizičke lokacije i objekata za smeštaj IT infrastrukture;
- angažovanje kontakt osoba i bezbednosnog osoblja za podešavanje;
- povećanje kapaciteta servera za skladištenje podataka i usklađivanje sa zahtevima skaliranja datih aplikacija;
- obezbeđivanje pomoćnog osoblja za održavanje infrastrukture;
- omogućavanje internet konekcije sa dovoljno propusnog opsega za pokretanje aplikacija;
- podešavanje mrežne infrastrukture, uključujući zaštitne zidove, balansere opterećenja, rutere i prekidače.

Ovo bi povećalo troškove i resurse, kojima se ne može upravljati, ostavljajući centar podataka samo kao rezervnu kopiju podataka i ništa više.



Slika 1. Koraci prilikom izrade plana oporavka od katastrofa [4].

Projekat Cloud Disaster Recovery nudi organizacijama nekoliko prednosti, uključujući sledeće [5]:

» ušteda vremena/kapitala;
» više opcija lokacije rezervne kopije podataka;
» jednostavan za implementaciju uz visoku pouzdanost;
» prilagodljivost.

Za organizacije koje po prvi put razmatraju oporavak od katastrofe u oblaku i pitaju se odakle da počnu u nastavku je jednostavan plan oporavka od katastrofe u oblaku koji može pomoći u osmišljavanju efikasne strategije oporavka od katastrofe:

Plan oporavka od katastrofe u oblaku – slika 1

Korak 1: Razumeti svoju infrastrukturu i predvideti sve rizike

Neophodno je uzeti u obzir IT infrastrukturu kompanije, uključujući imovinu, opremu i podatke koje kompanija poseduje. Takođe je važno proceniti gde se sve to čuva i koliko sve to vredi. Kada se završi sa procenom imovine, potrebno je procenti rizike koji mogu uticati na sve ovo.

Rizici mogu uključivati prirodne katastrofe, krađu podataka i nestanke struje između ostalog. Kada se izvrši ova procena, kompanija je u boljoj poziciji da osmisli svoj plan za Disaster Recovery Plan (DRP) kako bi eliminisala/minimirala ove rizike.

Korak 2: Sprovođenje analize poslovnog uticaja

Analiza uticaja na poslovanje je sledeća na listi. Ovo će kompaniji omogućiti razumevanje ograničenja njenog poslovanja kada dođe do katastrofe.

Sledeća dva parametra pomažu kompaniji da proceni ovaj faktor:

» ciljno vreme oporavka (RTO);
» ciljna tačka oporavka (RPO);

Parametri koji procenjuju rizik od gubitka podataka su:

a) Ciljno vreme oporavka (RTO)

RTO je maksimalno vreme u kojem data aplikacija može da ostane van mreže pre nego što počne da utiče na poslovanje.

Scenario 1: Ako je kompanija posvećena brzom pružanju usluga, onda kvar aplikacije može da je košta mnogo. Štaviše, moraće mnogo da uloži u DR plan da bi nastavila sa poslovanjem za nekoliko minuta.

Scenario 2: Ako kompanija ima posao srednjeg tempa i katastrofa utiče na njeno poslovanje, i dalje može pronaći alternativne načine za obavljanje poslovnih operacija. Stoga može podesiti svoj RTO na jednu nedelju. U tom slučaju neće morati da ulaže mnogo resursa u uštedu za oporavak od katastrofe, čime će uštedeti dovoljno vremena za nabavku dovoljnih rezervnih sredstava nakon katastrofe. Poznavanje sopstvenog RTO je veoma važno, jer je ekvivalentno broju resursa koje mora da uloži u svoj DR plan i jer se vreme izgubljeno u RTO može iskoristiti za prikupljanje rezervnih resursa.

b) Ciljna tačka oporavka (RPO)

RPO je maksimalno vreme u kome je moguće podneti gubitak podataka iz date aplikacije usled velike krize. Tačke koje treba uzeti u obzir za određivanje RPO [1]:

» mogući gubitak podataka kada dođe do katastrofe;
» mogući gubitak vremena pre kompromitovanja podataka.

Ako se primeni gore navedeni scenario 1, RPO može trajati samo pet minuta, jer je poslovanje kompanije kritično i ne može sebi priuštiti više od navedenog vremenskog intervala. Za scenario 2 će kompanija možda želeti da napravi rezervnu kopiju svojih podataka, ali pošto podaci nisu vremenski osetljivi, neće morati mnogo da ulaže u DR plan.

Korak 3: Kreiranje DR plana na osnovu RPO i RTO

Sada kada je kompanija odredila svoj RPO i RTO, može fokusirati na dizajniranje sistema koji će ispuniti ciljeve DR plana. Može birati između dolenavedenih DR pristupa za implementaciju DR plana [3]:

» pravljenje rezervnih kopija i vraćanje u prethodno stanje;
» Pilot Light Approach;
» toplo stanje pripravnosti;
» potpuna replikacija u oblaku;
» Multi-Cloud opcija.

Moguće je koristiti kombinaciju ovih pristupa u svoju korist ili isključivo u skladu sa sopstvenim poslovnim zahtevima.

Korak 4: Pristupanje pravom partneru u oblaku

Nakon što je razmotren pristup, sledeći korak bi trebalo da bude traženje pouzdanog dobavljača usluga u oblaku koji će pomoći u primeni. Ako kompanija planira da koristi punu replikaciju u oblaku, onda verovatno želi da uzme u obzir sledeće faktore da bi procenila idealnog dobavljača oblaka [5]:

» pouzdanost;
» brzina oporavka;
» upotrebljivost;
» jednostavnost podešavanja i oporavka;
» prilagodljivost;
» usklađenost sa sigurnošću;
» faktori za procenu idealnog dobavljača oblaka.

Svi veliki dobavljači usluga u oblaku, uključujući AWS, Microsoft Azure, Google Cloud i IBM, imaju opcije oporavka od katastrofe. Pored ovih velikih firmi, postoje i srednje i male firme koje nude kvalitetan oporavak od katastrofe kao uslugu (DRaaS).

Korak 5: Izgraditi svoju Cloud DR infrastrukturu

Nakon konsultovanja sa partnerom za DR u oblaku, kompanija može da radi sa dobavljačem na implementaciji sopstvenog dizajna i podešavanju DR infrastrukture. Na osnovu DR pristupa koji kompanija odabere, postoji nekoliko logističkih aspekata koje treba razmotriti [2]:

» Koja je količina infrastrukturnih komponenti koja će kompaniji biti potrebna?
» Na koji način će kopirati podatke u oblak?
» Koji su najbolji načini za pristup autentifikaciji korisnika i upravljanju pristupom?
» Koje će bezbednosne mere kompanija preduzeti da bi smanjila verovatnoću katastrofa?

Uvek treba imati na umu da je ključno osigurati da je DR strategija kompanije usklađena sa njenim RTO i RPO specifikacijama za nesmetano poslovanje.

Korak 6: Staviti plan oporavka od katastrofe na papir

Važno je imati standardnu smernicu ili dijagram toka procesa sa specifičnim uputstvima za svakoga ko je uključen u DR. Kada dođe do katastrofe, svaki pojedinac treba da bude spreman da preuzme odgovornost u skladu sa svojom ulogom u DR procesu. Štaviše, svako uputstvo treba da bude jasno navedeno na papiru, sa navedenim najsitnijim detaljima. Ovi koraci obezbeđuju delotvornost DR plana.

Korak 7: Često testiranje svog DR plana

Nakon stavljanja DR plana na papir, sledeći korak bi uključivao testiranje tog DR plana, i to često. Ovo pomaže da se osigura da nema rupa. Na papiru plan može izgledati kao najsveobuhvatniji, ali kompanija može saznati kolika je njegova kredibilnost tek nakon testiranja.

Zaključak

U ovom radu smo pokazali koliko računarstvo u oblaku postaje važno u svakodnevnom životu. Samim tim se velika većina kompanija zasniva na računarstvu u oblaku. One moraju biti dovoljno svesne katastrofa u oblaku. Kada dođe do katastrofe, onda se sve kompanije suočavaju sa velikim gubitkom, kako sa finansijskim gubitkom tako i sa gubitkom podataka, zbog čega su uvedeni mnogi mehanizmi oporavka.

Nedavna istraživanja pokazuju kolika je važnost postojanja DR plana, a u prilog tome ide podatak da svaki dolar uložen u ublažavanje rizika, kao što je DRP, štedi kompaniji četiri dolara gledano na duže staze. Stoga je jasno da bi svaka kompanija koja drži do svog poslovanja, pa i statusa, trebalo, ozbiljno da pristupa DRP, a možda i morala, kako bi osigurala svoju najvažniju imovinu, a to su podaci.

Literatura

1. Abedallah Z. A., Alwan A. A., Gulzar Y. Disaster Recovery in Cloud Computing Systems: An Overview. International Journal of Advanced Computer Science and Applications; 2020; 11(9): 702–710.
2. Fox R. & Hao W. Internet Infrastructure: Networking, Web Services, and Cloud Computing. CRC Press Taylor & Francis Group. 2018. ISBN: 978-1-1380-3991-9
3. https://cloud.google.com/architecture/dr-scenarios-planning-guide (pristupano: 8. 1. 2022)
4. https://see.asseco.com/banking-and-finance/security-other-services/infrastructure-services/disaster-recovery-as-a-service-draas-607/ (pristupano: 8. 1. 2022)
5. Jaiswal V., Sen A., Verma A. Integrated Resiliency Planning in Storage Clouds. IEEE Transactions on Network and Service Management; 2014; 11(1): 3–14.