Sinteza
Međunarodna naučna konferencija Univerziteta Singidunum

Impact of Internet on Business Activities in Serbia and Worldwide
Uticaj Interneta na poslovanje u Srbiji i svetu

DOI: 10.15308/SINTEZA-2014-635-641

KONTINUIRANO POSLOVANJE I OPORAVAK OD KATASTROFA I IZAZOVI SOLARNOG UDARA NA SRBIJU

Igor Lavrnić, Dejan Viduka
Singidunum Univerzitet, Srbija

Abstract:
Kolaps sistema snabdevanja električnom energijom, kao posledice solarnog udara, može paralizovati naciju na duži vremenski period. U ovom radu ćemo objasniti kako Kontinuiirano poslovanje i Oporavak od katastrofa-KPOK (engl. Business Continuity and Disaster Recovery) mogu da se nose sa ovim izazovom. Vreme koje je potrebno za potpunu revitalizaciju sistema distribucije električne energije, zavisi od stepena oštećenosti opreme i specifičnosti opreme, vezano za njenu nabavku. Većina opreme za elektrodistribuciju ne proizvodi se u Srbiji i za njenu nabavku potrebno je vremenski čak i do godinu dana i više. Suština ovog dokumenta je registrovano iskustvo zemalja koje su imale solarni udar, analiza konsekvenci po njihovu nacionalnu infrastruktutu, esencija zaključaka koje su te zemlje donele i mere koje su preduzele da bi sanirale katastrofu. Ovaj rad se više fokusira na posledice solarnog udara na nacionalne infrastrukture i kako Kontinuirano poslovanje i oporavak od katastrofa, kao naučna oblast, može da odgovori ovom izazovu, nego što objašnjava genezu solarnog udara.

Key words:
solarni udar,
nestanak električne energije,
Strategija kontinuiranog poslovanja i oporavka od katastrofa.

UVOD

Kontinuirano poslovanje i oporavak od katastrofa (KPOK) često predstavlja politiku očuvanja poslovanja jednog preduzeća; primarno fokusirajući se na zaštitu baza podataka sa ciljem očuvanja kontinuiteta poslovanja, kao i revitalizaciju poslovanja posle katastrofa. Ova oblast ne bi imala implikacije na celu državu, da Srbija nije prošla kroz proces IT revolucije, gde se preko 90% podataka od nacionalne važnosti čuva u elektronskom obliku. Direktna pretnja poslovnom kontiunitetu jedne države, podrazumevajući pre svega opasnost smanjenja operativnosti infrastruktura od nacionalnog značaja (elektrodistribucija, telekomunikacija, vodovod itd.), kojim upravljaju različiti operativni sistemi, predstavlja kolaps sistema. Dodatnu pretnju donosi i onesposobljavanje države da putem svoji E-servisa opslužuje građane,što predstavlja globalno ugrožavanje stanovništva. Čovečanstvo ima hiljade godina iskustva sa zemljotresima, poplavama, uraganima, a samo jedan vek sa solarnim udarima. Naravno, moramo uzeti u obzir, da nekoliko poslednjih (koji su se se desili u poslednjih 20 godina) čine 90% naučne osnove za studiranje posledica, za razliku od događaja koji su se desili početkom veka, kada elektronika nije ni postojala. Događaji koji čine osnovu istraživanja su sledeći:

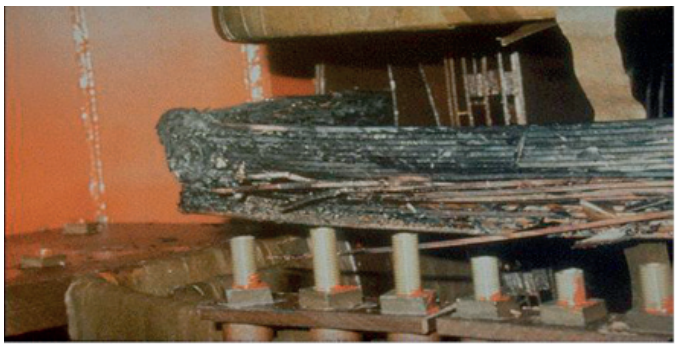
- ″Carington Event″ , 1859 (SAD)
- ″Hydro-Quebec Event″ 1989 (Kanada)
- ″Haloween Storm 2003″ (Švedska i Južna Afrika)

Mnogo veće i ekonomski snažnije zemlje (SAD, Kanada i Švedska) nisu mogle da saniraju posledice solarnog udara u kratkom vremenskom roku,što otvara novo pitanje: koliko je Srbija spremna da odgovori takvom izazovu? U svakom slučaju, kompletna priprema za odbranu od solarnog udara podrazumeva i značajna ulaganja u elektroprivredu, kao i alternativne izvore energije u slučaju dugotrajnog nestanka struje. Pored toga, *sve nacionalne infrastrukture* bi trebale dodatno investirati u prezervaciju baza podataka, siteme upravljanja i komunikacije. Ova ulaganja sa dosadašnje tačke gledišta izgledaju nepotrebna, jer Srbija do sada nije dožvela solarni udar. Bitno je pomenuti činjenicu da se solarni udar do sada isključivo dešavao državamo koje su bile iznad 50° severne ili južne geografske širine, što se u poslednje vreme menja usled pomeranja Severnog pola ka Sibiru, tako da se solarni udar dogodio u Južno Afričkoj Republici koja je takođe ispod 50°, ali južne geografske širine (mora se uzeti u obzir da je je Srbija locirana ispod 50° severne geografske širine).

SOLARNI UDAR I NJEGOVE POSLEDICE

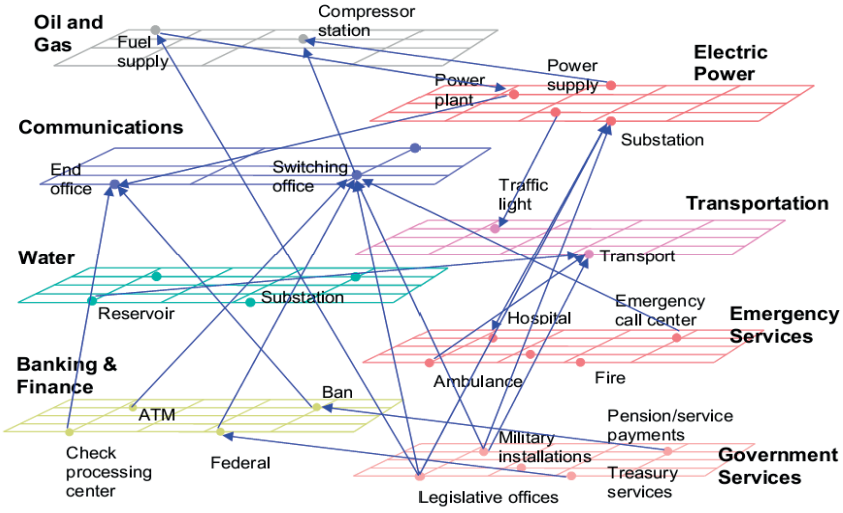
Većina solarnih oluja proizvodi minorne efekte na zemlji.Tipično je da se mogu očekivati kratkotrajni nestanci električne energije, prekid komunikacija, kolaps navigacije u vazdušnom saobraćaju, gubitak nekoliko satelita i prelepa pojava na nebu zvana “Aurora Boreas”. Ali sa

povećanjen inteziteta solarnih oluja, povećava se i kapacitet stvaranja katastrofa većih razmera koje mogu biti i regionalnog karaktera. Oštećene elemente distributivne mreže električne energije, je teško nabaviti u kratkom vremenskom roku, uzimajući iskustva nekih bogatijih zemalja (BDP per capita, pokazatelj)[1]. Shvatili smo da je potrebno nekoliko meseci da se nabave delovi, zbog svoje unikatnosti i nepostojanja zaliha istih (pogledati Prikaz br.2).



Prikaz 2: Bliži pogled na delove transformatora koji su oštećeni tokom solarnog udara u Salem nuklearnoj elektrani.

Problem i jeste u tome što će prozvođači biti pretrpani porudžbinama i neće moći da odgovore svim zahtevima u kratkom vremenskom periodu, što ostavlja naciju u fazi kolapsa nedeljama, mesecima, pa možda čak i vise od godinu dana. (Thorberg.R;2012) [2]. Dugotrajan nestanak električne energije dovešće do kolapsa snabdevanja vodom, kolapsa kompletne proizvodnje u svim industrijskim granama (osim poljoprivrede), trgovine, bankarstva, saobraćaja, komunikacija, a tokom zimskog perioda, stvara se problem grejanja u gradovima (pogledati Prikaz br.1). Solarne oluje imaju dosta sličnosti sa ostalim prirodnim katastrofama (uraganima, zemljotresima, cunamijima) upravo po katastrofalnim posledicama koje proizvode i zbog toga predstavljaju visoko rizičnu kategoriju po bezbednost nacije, ako nisu pravilno sanirane. Pogotovo je rizično slabljenje zemljine magnetosfhere, koja je intezivno oslabila u poslednjih 200 godina, po nekim izvorima 10% (Evropska Svemirska Agencija. SWARM Project, 2014)[3].



Prikaz br.1: Međusobne povezanosti infrastruktura jedne države tokom prekida sanbdevanjem električnom energijom

KAKO SE PRIPREMITI ZA SOLARNI UDAR

Ono na šta se želimo posebno fokusirati u ovom radu, jesu instrukcije nadležnim organima da urade sledeće:

- Organizuju izgradnje novih skloništa sa vodenim pojasom i urade adaptacije postojećih u lokalnim zajednicama;
- Osnuju vladine agencije koje će organizovati i kordinirati sve aktivnosti, edukovati i savetovati građane kako da prežive tokom solarnog udara;
- Organizuju bolju pripremu elektro distributivnih sistema u državi;
- Organizuju bolju zaštitu podataka od elektromagnetnog udara i obezbede rezervne izvore napajanja električnom energijom;
- Organizuju život u velikim gradovima tokom dugotrajnog nestanka napajanja električnom energijom;

KPOK I SOLARNI UDAR

Kontinuirano poslovanje i Oporavak od katastrofa (KPOK) kao oblast koje treba da organizuje kompanije da se što bolje pripreme za slučaj nastanka akcidenta, se posebno ukršta u svojim naučnim pravcima sa snabdevanjem električnom energijom, IT sistemima, sistemima za komunikaciju, edukacijom zaposlenih u svim gore pomenutim institucijama kao i ostalim oblastima koje se ne bave informacionim tehnologijama. Oporavak od katastrofa je tipičan nastavak naučne oblasti Kontinuiranog poslovanja, gde se kompanija ili državna institucija, koja je već napravila repliku kompletnog IT sistema na sigurnoj lokaciji, kroz ovu naučnu oblast edukuje kako da povrati kontiuitet poslovanja posle nastale katastrofe. Na prikazu povezanosti svih infrastruktura jedne države (videti prikaz br.1), jasno se vidi kompleksnost i međusobna zavisnost svih infrstrukura jedne države tokom nestanka električne energije. Mnoge kompanije kontinuirano zavise od IT sistema, baze podataka, softverskih aplikacija koje su prilagodile za svoj posao, mađutim ozbiljniji pristup očuvanju vitalnosti svog elektronskog poslovanja imaju samo banke i velike kompanije, koje su to iskustvo prenele iz svojih matičnih zemalja. Ex-Yu republike uključujući i Srbiju, su posredstvom EU uglavnom donele (ili su još u procesu donošenja) potrebnu regulativu u svoj pravni sistem koji reguliše ovu oblast, uglavnom kroz zakon o zaštiti tajnosti podataka i sajber strategiju. Ogromni su rizici koji se nose sa zenemarivanjem ove činjenice i ogledaju se uglavnom u sledećem:

- Izgubljen profit; gubitak samo jedne od IT podrške kao što su E-mail i internet, mogu kompaniju koštati određenu sumu novca, da ne spominjemo E-Banking ili ostale aplikacije koje prate berzansko poslovanje, tu se već govori o milionima evra.

- Poverenje klijenata; kada se kompaniji i vladinoj instituciji dogodi prekid poslovanja ili još goregubljenje baze podataka, klijenti mogu izgubiti poverenje u takvu instituciju, i gubici u narednom periodu mogu se udesetrostručiti.
- Okruženje haosa; državne institucije kao što su Vojska, Policija, Pravosuđe, Socijalno osiguranje i Bankarski sistem mogu paralizovati naciju. Konkretno, ako dođe do solarnog udara, niko od stanovništva neće biti spreman da dočeka takvu katastrofu. Paralizovan saobraćaj u velikim gradovima, kolaps banaka, pumpi za snabdevanje gorivom, su prvi izazovi sa kojim se stanovništvo mora suočiti. (The CISSP Prep Guide Gold Edition 2003) [4].
- Ako nestanak struje potraje duže vreme (a moguće je, s obzirom na pripremljenost elektrodistribucije za ovakve situacije), dolaze novi problemi. Ono što sledeće predstavlja problem je rad komunalnih službi, opšti kolaps svih vladinih institucija, nemogućnost pružanja zdravstvene pomoći, nemogućnost snabdevanja hranom i vodom.

Zaposleni i njihova efektivnost u ovakvim situacijama; Kako je tehnologija dovela do toga da je postala veliki deo savremenog poslovanja i da zaposleni ne mogu bez postojeće tehnologije i aplikacija da budu produktivni.

Sve ove gore pomenute stvari su esencijalne Potrebno vreme oporavka (PVO) u engleskoj verziji ″Recovery Time Objective (RTO)″, što podrazumeva koliko brzo kompanija ili vladina institucija može da se oporavi i da počne sa normalnim radom. Pored toga veoma bitna jeste i Prelomna tačka oporavka (PTO) u izvornoj engleskoj verziji ″Recovery Point Objective (RPO)″, što podrazumeva koliko je spremna kompanija, ili vladina institucija da izgubi od podataka, da bi što pre počela sa radom. Savremeni menadžment kompaija, koji je edukovan na zapadu i funkcioniše po zapadnim principima i moralnim načelima,upoznat je sa činjenicom da je Plan oporavka od katastrofe (POK) potreban, a posebno će biti forsiran od strane menadžera koji dolaze iz zemalja koje su već imale iskustvo sa nesrećama većih razmera. (The CISSP Prep Guide Gold Edition 2003) [4]. Pozitivan primer je dala Narodna banka Srbije (NBS) koja je kroz regulacione akte, kojima reguliše poslovanje banaka (NBS odluka o upravljanju rizicima banke 64-72) [5] , direktno uvela ISO 22301 standard u implementaciju. Po nezvaničnim podatcima jedina banka koja je u potpunosti ispunila zadatak je Banca Intesa AD, dok su ostale banke to više uradile formalno, uvodeći ″ Cold Site″-ove, odnosno prostorije u kojima bi trebalo da postoje ″Shadowing″ baze podataka. Međutim ″Cold Site″ podrazumeva da ″back-up″ baze nisu aktivne, da nema alternativnih sistem napajanja, grejanja i hladjenja, što praktično znači da bi u slučaju akcidenta banka pretrpela ogromne gubitke, jer bi mogla da izgubi kompletnu bazu podataka. Oporavak od ovakvog gubitka trajao bi nekoliko meseci do godinu dana, dok bi se usposatvili novi sistemi i izvršio unos iz arhive u baze podataka. Praktično to bi značilo da bi ogromna većina klijenata napustila dotičnu banku i prešla sa poslovanjem kod one banke koja bi bila odmah operativna. Pored toga ako bi klijenti kod nove banke bili zadovoljni nivoom usluge, to znači da bi tu i ostali kao klijenti, što dalje vodi do kolapsa banke koja nije bila spremna da odvoji sredstva za KPOK, jer je njen menadžment smatrao da je to manje važna investicija.

PLANIRANJE KPOK-A

Održavanje Plana kontinuranog poslovanja i oporavka od katastrofa (KPOK) je tekući proces koji zahteva više od jednogodišnje provere, upravo zbog promena koje se u IT dešavaju veoma dinamično. Postoji 5 ključnih faza koje čine životni ciklus oporavka od katastrofe, a one su :

- Analiza; ovo je najkritičnija faza u razvoju KPOK plana, upravo zbog osetljivog segmenta analize, koja treba da odredi koje su slabe tačke kompanije, definiše moguće pravce udara,opasnosti i scenarije udara na kompaniju;
- Kreiranje rešenja; tokom ove faze apsolutni imperativ ima zadatak da se pronađe što efektivniji model sa stanovišta cene koštanja, kao da se naspram toga pronađe tehnički održivo rešenje;
- Implementacija; ova faza se isključivo sastoji od sprovođenja u delo svega što je u prethodnoj fazi kreirano;
- Testiranje provera prihvatljivosti; da bi se sa sigurnošću utvrdilo da je kreiran KPOK plan prihvatljiv za kompaniju sa stanovišta njihovih potreba , mora se izvršiti testiranje;
- Održavanje; jedno kada se KPOK plan ustanovi kao deo poslovne politike kompanije ili vladine institucije, održavanje je neophodno sa stanovišta vitalnosti celog koncepta.

  Održavanje je tekuća faza koja zahteva kontinuirano održavanje vezano za IT tehnička rešenja, rešenja oporavka od katastrofa i organizacionih promena koje imaju direktan uticaj na operativnu pripremljenost.

Tokom celog životnog veka kompanije KPOK uvek mora čuvati kompaniju od potencijalnih operativnih rizika i održavati kontinuiranu vitalnost celog koncepta. Kada se desi najgori scenario i postane udarna vest na naslovnim stranama novina, pripremljenost kroz KPOK će omogućiti kompaniji da prevaziđe problem i da stekne ogromnu prednost nad konkurencijom, dok vladine institucije stiču veliko poverenje svojih građana. (The CISSP Prep Guide Gold Edition 2003) [4]. Primarna uloga plana kontinuiranog poslovanja jeste u redukciji rizika od potencijalnih finansijskih gubitaka kao i u stvaranju sposobnosti da kompanija ili vladina institucija momentalno nastavi da normalno funkcioniše.

U ovome delu rada ćemo više objasniti koji pristup ima plan kontinuiranog poslovanja prema delovima u kojima se procesiraju kritične informacije,i hardverskim delovima koji su veoma bitni za ceo KPOK uopšteno, a to su:

- Napajanje strujom;
- LAN,WAN i serveri;
- Telekomunikacione i poprečne veze;
- Radne stanice i radni prostor;
- Aplikacije, softveri i podaci;

- Baze podataka;
- Dužnosti zaposlenih i procesi;

Apsolutni prioritet KPOK-a su ljudski životi. Evakuacija zaposlenih, omogućavanje građanima da i u slučaju vanrednih situacija mogu nesmetano korisiti sve resurse državne infrastrukture, treba da bude nacionalni imperativ. Glavni cilj planiranja oporavka od katastrofa je da obezbedi organizovan način donošenja odluka tokom akcidenta, kao redukcija konfuzije sa ciljem povećanja efikasnosti. Rukovodeći se iskustvom velikih katastrofa koje su se desile gotovo na svim kontinentima, oporavak od katastrofa kao naučna oblast insistira da se plan napravi pre akcidenta, a ne tokom katastrofe na licu mesta. Upravo zbog svega već pomenutog potrebno je dosta testirati plan,da bi se odredio kapacitet kompanije. Ciljevi planiranja oporavka od katastrofa su brojni ali podjednako važni, i uključuju sledeće oblsti:

- Organizovanje zaštite napajanja električnom renergijom (kompanije: gasni ili dizel generatori, država: elektroprivreda)
- Svođenje kašnjenja funkcionisanja vitalnih funkcija kompanije ili države na najmanju moguću meru
- Testiranje i baždarenje sistema koji treba da omoguće gore pomenuto
- Svođenje potrebnog vremena za donošenje odluka menadžmenta za vreme akcidenta, na najmanju moguću meru, jer su sve opcije već isiptane i testirane

Proces Planiranja oporavka od katastrofa, uključuje kreiranje i razvijanje plana, koji je identičan procesu izrade Plana za kontinuirano poslovanje. Faze u izradi Plana oporavka od katastrofa su sledeće:

- Planiranje ″backup″-ovanja svih servisa i svih bitnih elemenata za sam Plan oporavka. U nastvaku ćemo navesti najčešće upotrebljavane delove ovog procesa:
  - Potpisani ugovori sa drugim kompanijama o međusobnom pomaganju u vreme akcidenta;
  - Strategija na nacionalnom i individulanom (nivou kompanije);
  - Uplaćeni servisi (u slučaju manjih akcidenata);
  - Čuvanje podataka u više centara (multiple shadowing);
  - Servisni biroi (u slučaju manjeg akcidenta);
  - Ostale alternativne verzije ″backup″-ovanja podataka;
- Reciprocalni ugovori; su ugovori o saradnji između dve kompanije, koje imijau slične potrebe i zahteve, vezano za očuvanje podataka, dosta je česta praksa u SAD i EU. Ovo konkretno znači da kompanije jedna drugoj rade ‘’shadowing’’ podataka. Potrebno je da obe kompanije imaju slične softverske i hardverske konfiguracije, da bi ovo moglo uspešno da se izvede.
- Ugovori sa provajderima ‘’Shadowinga’’; Ugovori sa provajderima ‘’backup’’-ovanja podataka je takođe jedan od modela, koji može da bude dobro rešenje u slučajevima manjih akcidenata.
  - Potpuno opremljena jedinica (Hot site) ovako opremljena jedinica za čuvanje podataka mora da ima generator, grejanje, ventilaciju i hlađenje (engleska skraćenica HVAC), i funkcionalnu ‘’file/print’’ radnu stanicu. Pored već navedenog obaveznog hardvera, radna stanica mora da ima softver za prebacivanje podataka, koji moraju biti kao ‘’ogledalo’’ servera njihovog klijenta. Pored toga, ova radna jedinica mora biti redovno administrirana,da bi se uverili da li je sve prekopirano za čuvanje sa klijentovog servera. Prednosti ovakve usluge su mnogobrojne, pored 24/7 usluge, suštinska prednost dolazi do izražaja tek u slučaju akcidenta.
  - Opremljena, ali ne i funkcionalna jedinica (Warm site) je u potpunosti isto opremljena kao ″Hot site″ ,samo što sistem nije aktivan i nije povezan sa glavnom bazom podataka.
  - Neopremljena jedinica (Cold site) ova jedinica ima napajanje električnom energijom, ventilaciju, grejanje, poprečne veze, ali nema ništa od hardvera i softvera. Ovo je najsiromašnija opcija, ali nažalost i najčešća. U ovoj opciji sva oprema treba da se kupi, ili donese iz matične firme.
  - Narodna banka Srbije kao što smo već pomenuli, uvela je standars KPOKa svim bankama, međutim, samo nekoliko banaka (među kojima je najviše uradila Banca Intesa AD) osposobila ″Hot site″, isto tako manji broj banaka je osposbio ″Warm site″,dok je većina osposbila ″Cold site″, čisto da bi ispunili obavezu koju je postavila NBS, (NBS odluka o upravljanju rizicima banke 64-72) [5].
- Koncept velikog broja centara;je deljenje svojih resursa na veći broj lokacija. Ovaj sistem može biti:
  1. ″In home″ odnosno u okviru firme (npr banka rasporedi ″backup″ delove svoje baze po filijalama)
  2. Udruži se veći broj firmi koji čuvaju baze jedni drugima.
- Servisni biroi; organizacije koje se profesionalno bave čuvanjem podataka, takođe mogu biti opcija (HP, IBM..)
- Ostale alternativne metode čuvanja baza podataka; predstavljaju kombinaciju svih gore pomenutih opcija, uključuje čak i mobilne baze podataka na kamionima koji imaj HVAC.

Kao i kod životnog osiguranja, ovo su procedure za koje se nadamo da ih nikada nećemo primenjivati. Primarni elementi procedura za oporavak od katastrofa su sledeći:

- Tim za oporavak; njegov primarni zadatak je da tehnički osposobi kritične tačke poslovanje preko jedinica u kojima su čuvane baze podataka.
- Tim za spašavanje; njegov primarni zadatak je da vrati poslovanje u normalu. Preporučuje se da za ovaj posao kompanija ili vladina organizacija angažuje drugi tim, odnosno da ne bude isti tim za oporavak i za spašavanje.

- Rekovalescencija u normalno poslovanje; prethodno postavljeni Plan oporavka od katastrofa, sada dolazi u proces realizacije. Proces normalizacije poslovanja treba takođe da bude rukovođen posbnim timom, koji će u uvaj proces uključiti i prethodno pomenuta dva tima.

PLAN OČUVANJA NAJVREDNIJIH RESURSA

Kompanija ili vladina organizacija, moraju nakon akcidenta da dođu do svojih dragocenih podataka bez kojih funkcionisanje ne bi bilo moguće. U ovom delu napravićemo pregled opcija za čuvanje podataka (The CISSP Prep Guide Gold Edition 2003) [4]. Dok se većina procedura odnosi na očuvanje podataka u elektronskom obliku, malo smo vremena posvetili očuvanju podataka koji se nalaze u štampanom obliku, a oni su podjednako važni , u nekim slučajevima i važniji od podataka u elektronskom obliku (npr važni potpisani ugovori). Upravo DCM omogućuje da se štampani dokumenti prenose u elektronski oblik, gde je čuvanje podataka mnogo lakše. U sledećem delu ovog poglavlja objasnićemo proces čuvanja dokumenata i modele čuvanja istih:

- Transfer dokumenata u elektronski oblik i njihova manipulacija; sam transfer dokumenta se obavlja skenerima, dok se u elektronskom obliku čuvaju na nekoj sigurnoj lokaciju. Oni dokumenti koji se često koriste i u svakodnevnom poslu, zadržavaju se u kompaniji;
- Softver i hardver za čuvanje podataka; ovde se koriste neki softveri koje često srećemo u svakodnevnom životu (Adobe Acrobat ili više profesionalniji EMC);
- Podatci čuvani na diskovima; u slučajevima gde se potreba za prostorom za čuvanje podataka drastično povećava, jedna solucija koja može da pomogne je i DAS (direct attached storage) koja se direktno kači na server. Takođe postoje i manje skupi diskovi kao što su SATA (serial advanced technology attachment) ili SAS (serial attached). Pored toga je moguće i kopiranje podataka i slanje preko WAN-a na druge lokacije da bi se oslobodio prostor za nove podatke;
- Trake za čuvanje podataka; čuvanje podataka na elektromagnetnim trakama je najekonomičniji način čuvanja podataka na duge staze. Zbog svoje cene sve je više u upotrebi, ali zato revitalizacija baze sa traka traje od 24 do 48 časova;
- Efektivnost, zaštita i arhiviranje; efektivnost čuvanja podataka u korelaciji sa cenom variraju od kompanije do kompanije, uzimajući u obzir da svaka kompanija ima svoje jedinstvene zahteve u dizajnu sistema. Zaštita podataka može biti u raznim varijatetima uključujući i onaj kombinacije trake i diska;
- DE-dupliciranje fajlova naspram arhiviranja; ovaj metod je odličan za kompresovanje i čuvanje podataka kod kojih nema potrebe za čestom upotrebom, kao što su arhive VM Ware ili VMDK fajlovi. Sa druge strane DE-dupliciranje nije preporučljivo sa aspekta KPOKa pogotovo za one fajlove kojima je potreban čest pristup;
- Hijerarhijski sistem čuvanja podataka (HSM); podrazumeva migraciju podataka iz kompanije u jeftinije modele čuvanja podataka, ali ostavlja za sobom ″Stub″fajl, koji opet omogućava aplikaciji ili fajlu da budu pronađeni u centarlnoj bazi podataka, međutim kada se fajl želi otvoriti u svakodnevnom poslovanju , on se povlači iz jeftinije baze;

MOGUĆI ODGOVOR SOLARNOM UDARU

Naučne oblasti koje se bave ovim fenomenom, kao i već postojeća inženjerska rešenja, treba da budu uključena, ali sa zadatkom da i dalje analiziraju fenomen i da pronalaze nova rešenja. Posebno treba obratiti pažnju na postojeća inženjerska rešenja u distribuciji električne energije, zaštiti elektronike od efekta EMP-a i zaštiti stanovništva od protonskih snopova koji mogu pojedinačno da probiju zemljinu magnetosferu i ugroze živote ljudi. (Thorberg.R;2012) [2]. Kao što je već poznato elektroditribucije će biti momentalno pogođene ekstremnom geo-magnmetičkom olujom, pošto su naučnici već radili na pronalaženju efikasnog načina da se ublaže negativni efekti, trebalo bi uraditi sledeće:

- Isključivanje sisteme pre solarnog udara, može sačuvati komponente elektroditributivne mreže, pogotovo transformatore. Ovo je moguće, zbog svemirske meterološke stanice koja je osnovana, kao i zbog dva satelita koja vrše opservaciju sunčevih aktivnosti. Realno posle jače erupcije sunca, ostaje nam 26 sati da se pripremimo za solarni udar; (Evropska Svemirska Agencija. SWARM Project, 2013)[3];
- Menadžeri elektro distributivne mreže mogu povećati kapacitet mreže, da bi mogla da izdrži udar;
- Vodovi visoke gustine, mogu biti zamenjeni vodovima niže gustine koji mogu bolje da podnesu solarni udar;
- Instaliranje blokatora u distributivnu mrežu, kao i neutralnih otpornika u transformatore značajno će smanjiti uticaj geomagnetičke indukcione struje;
- Katodna zaštita je tehnika koja se često koristi za kontrolu korozije metalnih površina, tako što ta površina postaje katoda elektrohemijske ćelije. Priključivanje dodatne metalne površine,više podložne korodiranju,koja deluje kao anoda, stvara uslove da ćelija radi.
- Kupovinom Emporiums transformer neutralnalih uređaja za blokiranje, koji blokiraju geomagnetske indukovane struje treba ih instalirati u elektro-distributivnu mrežu,
- Instaliranje Varistors-a od metalnog oksida, koji se pružaju prenaponsku zaštitu;
- Obezbediti da fabrike vode imaju generatore u cilju održavanja snabdevanje vodom . Obezbediti benzinske stanice generatorima u cilju pružanja normalnog snabdevanja gorivom;

Vladine regulative trebaju da povećaju, nivo zaliha rezervnih delova elektrodistribucije, naročito delova za koje se već zna da mogu da budu oštećeni tokom solarnog udara (Thorberg.R;2012) [2]. Vazdušni saobraćaj treba da bude ograničen u delu gde je došlo do solarnog udara. Sistemi komunikacije su takođe podložni kvarovima usled delovanja geomagnetičkog udara. Radari i radio stanice su imali velike probleme tokom solarnog udara. Najbolje bi bilo da oni budu isključeni tokom visokog nivoa elektromagnetnog zračenja, da bi se pre svega sačuvale komponenente unutar uređaja. Urgentni centri, velike bolnice, policija, sudstvo, sigurno treba da razviju rezervni sistem napajanja preko gasnih generatora. Ono što je još jako bitno u haosu koji može da izazove dugotrajan nestanak struje, jeste pristup stanovništva svom novcu u bankama, kao i snabdevanje gorivom na benzinskim stanicama. Ovaj problem može država veoma lako da reguliše nizom mera u zakonima za vanredne situacije. Država treba da organizuje migraciju stanovništva iz gradova u manja mesta i sela, zbog lakseg snabdevanja vodom i hranom. Naravno, da nije dovoljno znati samo kako izbeći katastrofu, mnogo veči zadatak je pronaći način za implementaciju ovih strategija u svakodnevni život, a jedan od načina da se to postigne su sledeće metode:

- Edukovati širu društvenu zajednicu, državne institucije i sistem civilne zaštite;
- Primeniti inženjerske sisteme u zaštiti ranjivih delova distribucoije gasa i električne energije, i podstaknuti velike kompanije da ih sprovedu u što kraćem roku;
- Država mora da osnuje Telo za saradnju sa Svetskom svemirskom vremenskom stanicom ;

Vladino telo za kordinaciju u slučaju solarnog udara primarno treba da se fokusira na sledeće:

- Identifikaciju i kreiranje mreže menadžera za vanredne situacije;
- Izgraditi nezavisne kanale za komunikaciju, koji neće biti zavisni od usluga operatera za telekomunikaciju, organizovati redosled aktivnosti koje svaki menadžer za vanredne situacije treba da uradi, da bi se katastrofa svela na najmanju moguću meru;

ZAKLJUČAK

Naučni doprinos ovog rada je pre svega u savetovanju šire društvene zajednice, da bolje organizuje sistem zaštite IT opreme u svim vitalnim infrastrukturama,da organizuje sistem civilne zaštite, naspram iskustava zemalja koje su preživele solarni udar. Apsolutni imperativ je čuvanje ljudskih života, zbog toga još jednom želimo se fokusirati na instrukcije nadležnim organima da urade sledeće:

- Osnivanje vladine agencije, koja će biti povezana sa Svemirskom vremenskom agencijom;
- Organizovanje izgradnje novih skloništa sa vodenim pojasom i adaptacija postojećih u lokalnim zajednicama;
- Povećanje nivoa obaveznih rezervi naftnih derivata,
- Organizovanje bolje pripreme elektro distributivnih sistema u državi;
- Organizovati bolju zaštitu podataka od elektromagnetnog udara, primenjujući znanja iz TEMPEST zaštite za sve vitalne infrastukture.
- Organizovanje života u velikim gradovima;
- Osmisliti strategiju alterativnog funkcionisanja bankarskog sistema, omogućiti građanima brz pristup svojim novčanim sredstvima na računima.
- Organizovati prevoz građana iz velikih gradova u unutrašnjost zemlje kod njihovih rođaka, gde je lakše snabdevanje vodom i namirnicama.
- Revitalizovati prehrambenu industriju, omogućiti snabdevanje građana besplatnom hranom i higijenskim sredstvima;
- Revitalizovati u svim delovima zemlje sistem medicinske zaštite i snabdevanje lekovima;

Sve ovo gore navedeno je preduslov da bi država pružila minimalni nivo zaštite svojim građanima, kao što smo već napomenuli, ekonomija će se revitalizovati kasnije, sve će se vratiti u normalu, ali izgubljeni životi neće. Veoma je bitno da se ne dočeka da solarni udar dođe na naslovne stranice, i da se tek tada počnu sanirati posledice. Zemlje koje su imale solarni udar, jasno su navele svoja iskustva, čiju esenciju treba prilagoditi i primeniti. Pogotovo treba obratiti pažnju na život običnog građanina u velikim gradovima, gde dugotrajan nestanak elektične energije, može da izazove ozbiljne probleme u svakodnevnom životu.

LITERATURA

[1] BDP, Bruto Društveni Proizvod kao pokazatelj; Wikipedia 2014;

[2] Thorberg.R;Risk analysis of geomagnetically induced current in power systems;Division of Industrial Electrical Engineering and Automation, Faculty of Engineering,LTH,Lund University,Lund;2012;

[3] European Space Agency, ESA, SWARM Project; http://www.esa.int/Our_Activities/Observing_the_Earth/The_Living_Planet_Programme/Earth_Explorers/Swarm/ESA_s_magnetic_field_mission_Swarm; 2014;

[4] The CISSP Prep Guide Gold Edition (2003) Wiley Publishing, Inc.; Ronald L. Krutz ,Russell Dean Vines;

[5] NBS, Narodna Banka Srbije,Odluka o upravljanju rizicima banke 64-72; 2012; http://www.nbs.rs/internet/latinica/20/index_kpb.html

PRIKAZI

[1] Prikaz međusobne zavisnosti državne infrastrukture u slučaju dugotrajnog nestanka električne energije (wiki;2013)

[2] Prikaz oštećenog dela transformatora u Salem Nuclearnoj elektrani (wiki;2007)

RECOVERY AND SOLAR ATTACK CHALLENGES AGAINST SERBIA

Abstract:
The power outage, as direct consequence of solar attack, could paralyze the nation for a long period of time. We will explain how Business Continuity and Disaster Recovery could deal with this challenge. Moreover the time required for full recovery of service would depend on both the disruption and damage to the electrical power infrastructure. Most of critical electrical power infrastructure components are not manufactured in Serbia, and their acquisition ordinarily requires up to a year, which electrical infrastructure could leave out of service for periods measured in months to a year or more. The core of this paper is the recorded experience of the previous solar attacks, analyzes of consequences and essence of conclusions and acts how to avoid the catastrophe. This paper is focusing on consequences of power outage on Serbian national infrastructures, and how Business Continuity could provide solutions to overcome the challenges.

Key words:
solar attack,
pover outage,
business continuity and
disaster recovery strategy.