ZAŠTITA PODATAKA U MALIM I SREDNJIM PREDUZEĆIMA

DATA PROTECTION IN SMALL AND MEDIUM ENTERPRISES

DRAGAN RADOVIĆ
Univerzitet „Alfa" u Beogradu, Fakultet za menadžment Novi Sad

ZORAN ČEKEREVAC
Univerzitet „Union" u Beogradu,
Fakultet za poslovno industrijski menadžment Kruševac

SVETLANA ANĐELIĆ
Visoka železnička škola strukovnih studija Beograd

EVELIN VATOVEC KRMAC
Univerza v Ljubljani, Fakultet za pomorstvo Portorož

Rezime: *Kao i velike korporacije, mala i srednja preduzeća se u velikoj meri oslanjaju na čuvanje svojih važnih podataka na sopstvenim serverima. Ograničeni resursi i ranjivost na upade čine da su mala i srednja preduzeća pod većim rizikom. Oslanjanje malih i srednjih preduzeća (MSP) na klasičan bekap svojih servera može da bude nepovoljno rešenje u planu oporavka od iznenadne katastrofe. Osnovni bekap u maloj meri pruža zaštitu, a periodično snimanje podataka na rezervnu traku može u MSP dovesti do ugrožavanja podataka i gubitka vremena u neprihvatljivim količinama. Ključ za brz oporavak i vraćanje u radno stanje je sveobuhvatan plan oporavka od katastrofa, koji uključuje i brz pristup kopiji podataka koja se neprekidno ažurira po tzv. sistemu „up-to-the-minute copy". U radu su analizirane mere koje MSP treba i može da preduzme u zaštiti podataka, uključujući i oblak-bazirana rešenja.*

Ključne reči: *Mala i srednja preduzeća, zaštita podataka, krizne situacije, tehnologija.*

Abstract: *Like the large corporations, small and medium-sized enterprises (SMEs) rely on storage of their important data on their own servers. The reliance of small and medium-sized enterprises on the classic backup of their servers may be an adverse decision in the recovery plan for sudden disasters. Basic backup provides protection to a small extent. Periodically recording data to a backup tape or disk may endanger SME's data and may lead toward the loss of time in unacceptable quantities. A prerequisite for a speedy recovery and return into the operational state is a comprehensive disaster recovery plan, which includes quick access to copies of the data that are constantly updated by the so-called system "up-to-the-minute copy". This work discusses measures that SMEs can and should take to protect data, including cloud-based solutions. Special attention is paid to the choice of data storage technologies and ways to simplify data protection.*

Keywords: *Small and medium businesses, data protection, crisis, technology.*

1. UVOD

Ako se razmatra zavisnost uspešnog poslovanja preduzeća od podataka, videće se da je u tom pogledu potpuno svejedno da li se radi o velikoj multinacionalnoj kompaniji ili o kompaniji sa malim brojema zaposlenih (mikro i mala preduzeća). Kod donošenja odluka u vezi poslovanja jedna i druga zavise od kvaliteta informacija (podataka) koje koriste u svom svakodnevnom radu. Problemi u korišćenju podataka mogu da nastanu iz sasvima jednostavnih razloga (nestanka električnog napajanja, krađe RS-a)pa do uzroka koji za posledicu imaju loše namere - hakerskih upada u sistem ili napada virusima. Mala i srednja preduzeća (MSP) srazmerno malo ulažu u stvaranje preduslova za osiguranje zaštite informacionog sistema i podataka. Mnoga MSP smatraju da nisu interesantna napadačima i da će ih napadi zaobići. Ova pretpostavka je potpuno neopravdana, jer „svaka roba ima svog kupca". Sveobuhvatnijim i sofisticiranijim napadima su uglavnom izložene velike kompanije koje intenzivno koriste Internet i na njemu baziraju svoje poslovanje, ali i napadači početnici negde moraju da počnu, a za to im mogu poslužiti slabije zaštićeni sistemi na kojima imaju realnije izglede da ostvare svoje namere. Zbog toga, menadžment MSP pri donošenju odluke o obezbeđenju efikasnog sistema zaštoite, nebi smeo da razloge identifikuje kao malo verovatne od hipotetičkog ili slučajnognapada, već problemu mora prići sa svom potrebnom ozbiljnošću. Jednom ostavljen nezaštićen prostor u sistemu može se tokom vremena pokazati kao veoma veliki propust sa ogromnim direktnim i indirektnim troškovima. Iako su problemi zaštite hardvera i zaštite od prekida napajanja električnom energijom danas lako rešivi, ni taj aspekt ne sme da ostane zapostavljen.

Kultura vođenja poslova u današnjim uslovima znatno se promenila u odnosu na nedavnu prošlost, pa su se i rizici promenili. Novi faktori poslovanja zahtevaju praćenje i analizu sve većeg broja podataka, pa i sve veći broj različitih podataka postaje kritičan u poslovanju. Pored toga, potrošači ne tolerišu duže prekide u poslovanju neke firme i u slučajevima kada poslovanje sa

kompanijom koja ima prekide u radu postane neudobno, okreću se drugim kompanijama koje nemaju prekide u radu. Normalno, prihvatljivo trajanje prekida u radu nije u svim slučajevima isto. Korisnik računara svako čekanje duže od tri sekunde i poruke tipa *„The server is busy. Please try later!“* oseća kao teško prihvatljive i, ako se to ponavlja, pokušaće da nađe alternativno rešenje.

Današnji izazovi u oblasti zaštite podataka predstavljaju značajan rizik za preduzeća svih veličina, ali najveći rizik predstavljaju za mala i srednja preduzeća. MSP često nemaju ni osoblje ni budžet koji obezbeđuju prihvatljiv oporavak. Često ni ne postoji plan oporavka, nema oporavka sajta, ili pak rezerva za oporavak sajta nije dovoljno daleko od primarne lokacije u slučaju prirodnih katastrofa.

MSP obično imaju sve svoje kritične podatke na jednom serveru. Ako server „padne“, zato što većina kancelarija zavisi od tog servera, on bi morao da bude pokrenut i u potpunosti obnovljen odmah. U protivnom se ceo sistem izlaže skupim posledicama. MSP kao i velike korporacije u regulisanim privredama podležu istim propisima kvaliteta i dostupnosti podataka kao i uslovima zaštite podataka. U SAD-u su postavljena vrlo konkretna pravila o dostupnosti, organizaciji i zaštiti podataka regulacionim aktima, kao što su npr: HIPAA, DOD 5015, FDA Part 11, Sarbanes-Oxley, SEC Rule 17..., a za prekršaje su predviđene veoma stroge kazne. U Srbiji je zakonska regulativa ove vrste još uvek u povoju, ali i ovde postoje važeći zakoni: Zakon o elektronskoj trgovini, Zakon o zaštiti podataka o ličnosti... Problem MSP je nedostatak novčanih sredstava za preduzimanje potrebnih mera. Pored toga, svaki poremećaj u novčanim tokovima često je i fatalan za MSP. U svom članku "A Small Business Approach to Computer Downtime", Adian Mak Dermot procenjuje da svaki incident može da košta mali biznis između $ 200 i $ 800 po incidentu i po RS. [1]

Microsoft® Windows® Small Business Server (SBS) omogućava u ograničenom obimu malim preduzećima mnoge funkcije koje koriste i velike kompanije:

- osnovne mrežne servise: DNS, DHCP,..., SSH
- Windows networking: deljenje fajlova i printera,
- Web server,
- FTP servise,
- server elektronske pošte, opciono i server baze podataka
- podršku za mobilne uređaje, kao i
- funkcije backup i restore.

Linux Small Business Server (LSBS) nudi uglavnom iste usluge kao i Microsoft Windows SBS, s tim što nudi i Wiki kao dokument menadžment sistem, kao i napredne mrežne alate – nmap, nagios i nessus. SBS i LSBS stavljaju na raspolaganje alate za kreiranje periodičnih rezervnih kopija. Međutim, oslanjanje na ugrađeni osnovni bekap za zaštitu svih baza, u hitnim slučajevima ili u slučajevima katastrofa može ostaviti posao oštećen zbog potencijalnih praznina u zaštiti. Trake i rezerva na disku mogu samo da vrate podatke do tačke poslednje dobre rezervne kopije, što je najverovatnije bilo na kraju radnog vremena prethodnog dana. Svi podaci uneti od poslednje dobre rezervne kopije biće izgubljeni. Ako je najnovija rezervna kopija nepotpuna ili oštećena, onda se koristi sledeća po redu najnovija rezervna kopija i gubi još više podataka itd. Pored toga, vreme oporavka servera pomoću bekap kopije je kraće od vremena ponovnog uspostavljanja normalnog poslovanja, jer podaci moraju biti vraćeni sa bekap medijuma na korisnički disk pre nego što se može iskoristiti.

U razvoju malih preduzeća uvek je neophodan optimizam da bi se postigli povoljni rezultati, ali kada se radi o zaštiti podataka uvek je isplativiji pesimistički pristup sa mnogo opreza. Prema izveštaju američke Asocijacije Malog Biznisa (Small Business Association – SBA) više od 99% svih firmi koje imaju zaposlene su mala preduzeća. Pri tome ona zapošljavaju 50% svih radnika privatnog sektora i pružaju skoro 45% od plata stanovništva. U EU MSP čine 99,8% od preko 19 miliona preduzeća i zapošljavaju 66% radno sposobnog stanovništva i ostvaruju 54% ukupnog obrta. Ipak, MSP su najranjivija u kriznim situacijama baš zbog toga što su mala.

Iako je rukovodstvima MSP teško da pobijaju značaj pripreme za poslovanje u kriznim situacijama, lako im je da odlože planiranje i implementaciju mera za krizne situacije zbog svakodnevnih problema i ograničenih resursa. SBA procenjuje da se 25 do 40% malih firmi gasi posle krizne situacije ili dužeg prekida poslovanja. U svetlu nedavnih iskustava vezanih za prirodne katastrofe i na situacije koje su se javljale posle njih, SBA naglašava da su se poslu vratile samo one firme koje su se dobro pripremile za krizne situacije.

Pri analizama poslovanja mala preduzeća treba stalno da se pitaju o sledećem:

- Da li je preduzeće spremno da se privremeno preseli?
- Da li postoje kopije i pristup vitalnim poslovnim podacima? (SBA preporučuje da se bekap podataka čuva na lokaciji koja je udaljena najmanje 80km daleko od sedišta firme.)
- Da li postoji pristup vitalnim poslovnim aplikacijama? (plate za hitne slučajeve, računovodstvo, pristup dobavljačima i resursima)
- Koliko podataka firma gubi u bekapima za vanredne situacije?
- Koliko brzo firma može da se oporavi od katastrofe?
- Koliko dugo će firma biti bez veze sa našim kupcima?

Opšti krizni scenario

Razlozi i trenuci nastanka kriznih situacija su veoma raznovrsni, kao i scenariji po kojima se kriza odvija. Jedna od bezbroj mogućih kriznih situacija mogla bi da se odvija po sledećem scenariju:

Dan D, 16 sati:

Glavni i jedini server u agenciji koja se bavi vođenjem knjiga nekoliko malih preduzeća je iznenada pao zbog nepoznatog kvara. Zaposleni pokušavaju da samostalno restartuju računar i da server vrate u prvobitno stanje. Posle neuspelih pokušaja, pošto nemaju ugovor o stalnom održavanju opreme, pozivaju servis koji treba da popravi sistem. Kraj je radnog vremena i niko iz pozvane firme nije u mogućnosti da izvrši popravku. Serviser

zapisuje simptome i obećava da će sutradan da izvrši popravku. Poslednji bekap urađen je u utorak u 23 sata i sačuvan. Podaci od srede nisu zabeleženi na serveru.

Dan D+1, 10 sati:

U optimističkom rešenju problema, radnik servisa je došao u agenciju i počinje da testira sistem. Testiranjem je utvrdio da je greška u hard disku i da je to jedini hard disk koji se nalazi u računaru. Ugrađuje novi hard disk, instališe OS i korisničke programe sa instalacionih diskova i sa poslednjeg upotrebljivog bekapa prebacuje podatke na hard disk. Posle toga testira rad servera, podiže ga i priključuje na mrežu, podiže mrežu i osposobljava je za rad. Posao završava u 17 sati. Sada su u serveru poslednji ažurni podaci od utorka u 23 sata. Podaci od srede su izgubljeni. Zato što su zaposleni na radnim stanicama deo posla mogli da urade „off-line“ podaci od četvrtka su delimično uneti u radne stanice, ali ne i u server. Neko od zaposlenih ostaje u firmi prekovremeno da unese podatke sa radnih stanica od srede i četvrtka.

Dan D+2, 9 sati:

Sistem spreman za rad. Zaposleni počinju da rekonstruišu podatke koji nisu bili sačuvani i nisu uneti u bazu prošle noći. Posao završavaju pre kraja radnog vremena i sistem je spreman za rad neposredno pre vikenda.

Ovo je praktično idealan slučaj opravke servera u slučaju kvara jedinog hard diska. Idealno je to što je serviser hardvera ujedno i serviser softvera, što ima potreban hardver i softver, što je bekap urađen i sačuvan u ispravnom stanju, što je deo podataka sačuvan u radnim stanicama i mogao da se prebaci na server. U ovoj situaciji izgubljena su praktično tri radna dana zbog pada servera.

Svaki drugi scenario je znatno nepovoljniji. Moguće je da servis nema odgovarajuće komponente i da treba da ih nabavi od proizvođača, da je bejkap neispravan i da treba uzeti neki stariji bejkap, da nema zaposlenog koji bi prekovremeno radio i unosio podatke u server ili da radne stanice ne čuvaju podatke koji su namenjeni serveru ili... U svakoj takvoj situaciji sistem bi mogao da se osposobi znatno kasnije, a troškovi bi znatno porasli. Ne treba ni pominjati kako pad servera u agenciji istovremeno utiče i na poslovanje kompanija čije knjige agencija vodi.

Zato je za svako MSP veoma važno da sagleda šta može da uradi da minimizuje rizik od nastanka ovakvih kriznih situacija.

2. MERE KOJE TREBA DA PREDUZME

Iako je prva misao rukovodstva MSP izbor odgovarajuće tehnologije, uvek treba prvo početi sa izborom pravih ljudi, politike i procedura. Nabavku opreme treba realizovati tek kada se jasno definišu sve potrebe sistema. Time će se uštedeti i deo sredstava, jer cene IT opreme neprestano padaju. U MSP teško je očekivati da postoji posebna služba za informatiku i zaštitu podataka. Mnogo je češći slučaj da MPS odredi jednog zaposlenog u preduzeću, kao osobu odgovornu za zaštitu podataka. Ta osoba je odgovorna za istraživanje mogućnosti zaštite, kupovinu softvera i hardvera, testiranje sistema i obuku korisnika. Ona ima i obavezu da dokumentuje procese, jer bi eventualni odlazak ili odsustvo te osobe moglo da dovede do velikog rizika za sistem.

Osoba odgovorna za zaštitu podataka bi na početku svog rada morala da okupi malu grupu koja je u potpunosti upoznata sa tehnologijom posla. Na taj način mogu da se utvrde stvarne potrebe sistema i eventualna slaba i kritična mesta sistema. U srednjim preduzećima tu grupu mogu da čine npr. direktori ili šefovi pojedinih službi ili odseka. U malim preduzećima umesto grupe često je dovoljno da osoba zadužena za zaštitu konsultuje vlasnika firme ili njenog izvršnog direktora. Odgovorna osoba mora da bude upoznata sa svim relevantnim zakonima i propisima koji imaju uticaj ili mogu da utiču na prioritete zaštite.

Na osnovu zahteva tehnologije posla i potreba korisnika osoba za zaštitu podataka u saradnji sa rukovodstvom firme definiše kritične aplikacije i polje zaštite. U većini MSP najčešće se zaštita fokusira na jednu ili dve aplikacije, pre svega zbog ograničenih sredstava. Na ovaj način se sa ograničenim sredstvima mogu postići dobri rezultati.

U cilju predviđanja potrebnih investicija u zaštitu

MSP U ZAŠTITI PODATAKA

potrebno je proceniti gubitke po jednom nastalom otkazu sistema. Ovo je veoma problematično u malom preduzeću koje tek ulazi u posao, jer ne raspolaže potrebnim podacima. U takvim slučajevima, kada ne postoji sopstveno iskustvo, kao orjentir mogu da posluže iskustva sličnih malih preduzeća. Orijentaciona cena koštanja jednog otkaza može se dobiti iz sledeće formule:

$$Co_1=(\Delta\tau_o + \Delta\tau) \cdot (n \cdot HR + LR)$$

gde su:

Co_1=orijentaciona cena koštanja po jednom otkazu sistema

$\Delta\tau_o$ = trajanje ispada iz rada

$\Delta\tau$ = vreme između dva uzastopna bekapa

n = broj zaposlenih koji je otkazom sistema

HR= prosečna časovna plata zaposlenog pogođenog otkazom sistema; Ova vrednost se sa zadovoljavajućom tačnošću može dobiti ako se ukupna mesečna plata zaposlenih u tom delu srednjeg preduzeća podeli sa njihovim ukupnim brojem radnih časova. U malim preduzećima se sa dovoljnom tačnošću može uzeti ukupna mesečna plata svih zaposlenih podeljena sa ukupnim brojem radnih časova svih zaposlenih.

LR= izgubljena dobit po času. Ona se može sračunati na različite načine, ali jedan od dovoljno dobrih pokazatelja bi mogla da bude dobit po času ostvarena u istom mesecu u prethodnoj kalendarskoj godini pomnožena koeficijentom rasta ostvarenim u tekućoj poslovnoj godini u odnosu na isti period u prethodnoj kalendarskoj godini.

Na veličinu potrebnih investicija u zaštiti podataka

značajno mogu da utiču željeno vreme oporavka aplikacije (VOA) i dopušteno vreme gubitka podataka (VGP). VOA se odnosi na zahtevano vreme u kom aplikacija treba da bude ponovo radno sposobna, a VGP se odnosi na vreme koje će biti prihvatljivo kratko da se ne izgubi mnogo od unetih podataka. Što su ova vremena kraća, mogu se očekivati veći troškovi. Sa rezultatima dobijenim procenom troškova treba upoznati rukovodstvo preduzeća koje će na osnovu toga doneti odluku o prihvatanju ili neprihvatanju predloženih mera i investicija.

3. BOR TEHNOLOGIJE ČUVANJA PODATAKA

Kada se definišu VOA, VGP i kada se definiše budžet, onda treba pristupiti izboru tehnologije kojom će se čuvati podaci. Vrlo lako se može zaključiti da nisu sve tehnologije podjednako dobre za svako MSP. Zbog razlika u načinima čuvanja podataka, pristupa podacima, trajnosti medijuma na kojima su pohranjeni podaci, brzine primo-predaje podataka, cene i drugih faktora (npr. način poslovanja preduzeća: jedna ili više lokacija), izboru odgovarajuće tehnologije treba pristupiti vrlo pažljivo.

Kod preduzeća koja posluju na više lokacija upotreba bekap magnetnih traka na mestu upotrebe može da bude rešenje ukoliko preduzeće raspolaže kadrom osposobljenim da briše i održava trake, da ih pravilno skladišti, redovno kopira i po potrebi vrši oporavak sistema. Pri ovome je neophodno da se obezbedi odgovarajuća radna disciplina i odgovarajuća redovnost u radu.

Mala i srednja preduzeća suočavaju se sa velikom dilemom:

- **trake kao rezervni sistemi** su prilično jeftine i pouzdane, ali nude skromne mogućnosti u pogledu VOA i VGP za kritične aplikacije. Uglavnom su neefikasne za udaljene lokacije.
- **hardverski miroring** koji koristi tehnologiju daljinskog kopiranja da obezbedi sinhroni miroring između dve lokacije nudi odlično VGP ali može da bude preterano skupo rešenje za MSP. Pored toga, ovo rešenje je daleko od idealnog za pravljenje rezervnih kopija sa udaljenih lokacija koje često imaju veze sa malim propusnim opsegom, a hardverski miroring zahteva velike protoke između lokacija.

Rešenja bazirana na asinhronim softverski baziranim replikacijama mogu da budu povoljna rešenja za MSP u pogledu VGP za kritične aplikacije. Pri tome se izbegavaju kompleksnost i visoka cena sinhrone replikacije. Kod softverski bazirane replikacije, menjaju se samo bitovi koji su promenjeni u procesu obrade podataka.

U poređenju sa rešenjima sa sinhronom replikacijom, ovaj pristup nudi niže opterećenje servera, brži apdejt i ispravke, kao i mogućnost da se replikacija vrši preko Internet mreže sa malim propusnim opsegom. Na softveru zasnovana rešenja replikacije mogu da obezbede oporavak servera i aplikacije sa odličnim VOA, tako da korisnici mogu da nastave da rade samo nekoliko minuta nakon pada sistema.

Izuzetno je važno da se podaci čuvaju i na rezervnoj lokaciji. Razlozi su brojni, a među njima su mogućnosti požara, poplave, zemljotresa, krađe i sl. Najpovoljnija varijanta je da se podaci čuvaju na lokaciji koja je stotinama kilometara udaljena od sedišta servera. Na taj način se mogu izbeći rizici od svih prirodnih katastrofa, požara i krađe. Ipak, ostaje problem zaštite podataka na toj udaljenoj lokaciji. Jedna od mogućnosti je i čuvanje podataka kod Internet provajdera, ili u prostorijama administratora mreže, ako administrator mreže obavlja svoj posao sa udaljene lokacije.

S obzirom na to da današnje cene hardvera ipak nisu visoke svi današnji serveri bi iz bezbednosnih razloga trebalo da obezbeđuju mogućnost rada bar po RAID 1 standardu**.** Po ovom standardu podaci se zapisuju na više (najmanje 2) identičnih diskova. Polje diskova obezbeđuje bezbedan rad u slučaju ispadanja ili kvara nekog hard diska i sistem normalno funkcioniše dokle god postoji bar jedan ispravan hard disk. Na ovaj način se u potpunosti izbegava pad sistema zbog neispravnosti jednog hard diska, ali se ne rešava problem potrebe za skladištenjem podataka izvan lokacije servera. Zbog razlika u obeležavanjima koja su se javljala kod različitih proizvođača računarske opreme uvedena je nova podela RAID sistema, tako da prema danas važećoj podeli kreatorima sistema zaštite podataka na raspolaganju stoje:

- disk sistemi otporni na kvarove (eng. Failure-resistant disk systems – FRDS)
- диск системи који толеришу кварове (eng. Failure-tolerant disk systems – FTDS)
- disk sistemi koji tolerišu katastrofe (eng. Disaster-tolerant disk systems – DTDS)

Sigurno je da su DTDS rešenja najbrža i najpoželjnija za upotrebu, jer omogućavaju neometan rad praktično u svim uslovima, ali su i najskuplja. Zato se koriste uglavnom tamo gde je važnost aplikacije izuzetna i gde je zbog toga i prihvatljiv visok trošak investicije.

4. KAKO POJEDNOSTAVITI ZAŠTITU PODATAKA

Očigledno je da mnoga MSP ne raspolažu dovoljno stručnim kadrom koji bi mogao da odmah reaguje u svim kriznim situacijama. Mnoga MSP za te poslove angažuju spoljne saradnike ili agencije, na principu mesečnog angažovanja ili angažovanja po potrebi. Zbog toga je zgodno da se, pored primene FRDS, FTDS ili DTDS rešenja, automatizuju operacije koje se redovno sprovode u cilju zaštite podataka. U tome su od velike pomoći proizvođači softvera.

Današnji operativni sistemi, a pogotovu serverski operativni sistemi, imaju mogućnost snimanja trenutnog stanja bilo u prethodno definisanim vremenskim intervalima, bilo na poseban zahtev korisnika, npr. pre instalisanja novog softvera. Ovo omogućava korisnicima

da na jednostavan način posle pada sistema dovedu sistem u prethodno zapamćeno ispravno stanje. Normalno, izmene unete posle zadnjeg snimljenog ispravnog stanja bivaju izgubljene. Teoretski, intervali između dva snimka stanja hard diskova mogu da budu i kratki, ali imajući u vidu da i snimanje stanja hard diskova ima neko svoje vreme trajanja, ove aktivnosti ipak ne treba izvoditi previše često, jer se upotreba računara time znatno usporava. U slučajevima kada su se desile neke neželjene promene u dokumentima, korisnik može jednostavnim pozivanjem poslednjeg ispravnog snimka hard diska da izabere željeni fajl, da pregleda njegove verzije i da izabere željenu verziju. Srećna je okolnost da i sam aplikativni softver pravi svoje rezervne kopije podataka, tako da se u slučajevima neplaniranog i neželjenog pada softvera veliki deo podataka može oporaviti.

Ovakav pristup eliminiše još jedan deo mogućih problema u zaštiti podataka, ali ne i sve preostale probleme zaštite podataka.

5. OBLAK-STRATEGIJA KAO MOGUĆE REŠENJE ZA MSP

„Oblak računanje“ je opšti naziv za sve što uključuje isporuku hostovanih usluga preko Interneta. Te usluge se u opštem slučaju mogu podeliti u tri grupe:

- Infrastruktura-kao-Usluga (***IkU***) (eng. Infrastructure-as-a-Service ***IaaS***)
- Платформа-као-Услуга (***ПкУ***) (eng. Platform-as-a-Service ***PaaS***)
- Softver-kao-Usluga (***SkU***) (eng. Software-as-a-Service ***SaaS***).

Naziv „*oblak računanje*“ inspirisan je simbolom u obliku oblaka koji se često koristi za predstavljanje Interneta u šemama i dijagramima. Poenta ideje je da se računanje ne sprovodi na korisničkom računaru, već u oblaku (negde na Internetu). Oblak-računanje predstavlja rešenja koja mogu da rade bilo gde, u bilo kom trenutku i sa bilo kog uređaja, bez potrebe da softver bude instaliran na korisnikovom računaru npr. na RS ili not-buku. Ovaj koncept je danas moguć, jer su ostvarene već relativno dobre veze korisničkih računara sa Internetom.

Ova strategija može da bude povoljno rešenje za MSP. Dovoljno je da MSP ima obične PC računare povezane sa Internetom i da svoje poslovanje obavlja uz pomoć provajdera koji se mogu nalaziti bilo gde u svetu. Pod pretpostavkom da je MSP izabralo dobre provajdere usluga, za uspešno funkcionisanje potrebna je još samo sigurna Internet veza. Računar koji se nalazi u prostorijama MSP može da bude bilo koji „tanki“ klijent, a ulogu servera dobija Internet, odnosno odgovarajući davaoci usluga. S obzirom da se radi o relativno novoj strategiji, mnogo malih i srednjih preduzeća se još ne odlučuje na prenos kritičnih aplikacija i podataka u oblak.

Jedan od razloga protiv strategije oblaka je pretpostavka da možda u nekom trenutku Internet neće biti dostupan, pa će biti nedostupne i baze podataka i aplikacije. Pored toga i visoki troškovi za postavljanje softvera i baza u oblak doprinose tome da kompanije ne koriste oblak usluge. Nasuprot tome, zaštita podataka i aplikacija predstavlja jedan od glavnih stimulansa malih i srednjih preduzeća da koriste oblak. Miroring podataka i aplikacija na različitim platformama oblaka i visok nivo redundanse usluga koju oblak nudi su jedna od ključnih preporuka za zaštitu podataka u oblaku. Oblak može da bude vrlo pristupačno rešenje za zaštitu kritičnih podatake i aplikacije, jer ispunjava praktično sve uslove za njihovo bezbedno čuvanje. bezbedno čuvanje. Pored zaštite podataka, mala i srednja preduzeća mogu da gledaju na oblak platforme i kao na širi nivo podrške, uključujući i mogućnost selidbe, upravljanja i nadgledanja oblak-bazirane IT imovine. Oblak-podržana rešenja za zaštitu podataka daju garanciju da preduzeća mogu da opstanu i ako njihova fizička IT infrastruktura pretrpi značajna oštećenja ili budu duže van pogona. Posedovanje takvih garancija je od ključne važnosti s obzirom na moguće posledice neadekvatne zaštite IT imovine. Prema procenama Contingency Planning, Strategic Research Corp. и DTI/Price Waterhouse Coopers, 70 odsto malih preduzeća koja dožive veliki gubitak podataka nestaju iz poslovanja u periodu do godine dana.[2] Već danas je ova koncepcija moguća i pristupačna MSP-ima. Usluge se mogu plaćati ili na osnovu članarine (fiksne pretplate) ili na osnovu utroška angažovanog resursa (kao npr. plaćanje utrošene električne energije).

6. ZAKLJUČAK

Novi faktori poslovanja zahtevaju praćenje i analizu sve većeg broja podataka. Zbog sve sveobuhvatnijih analiza i oštre konkurentske borbe na tržištu, sve veći broj različitih podataka postaje kritičan u poslovanju. Neki podaci su neophodni u odvijanju svakodnevnih aktivnosti i kao takve treba ih čuvati da bi bili uvek dostupni. Neki od podataka se smatraju tajnom preduzeća pa zbog toga zahtevaju i posebne mere zaštite. Deo podataka je namenjen okruženju u reklamne i druge svrhe i kao takav treba da bude dostupan svima u neizmenjenom obliku. Takvi sadržaji zahtevaju opet zaštitu, ali sa drugog aspekta. Zbog raznolikosti zahteva i sama zaštita je veoma različita od situacije do situacije. MSP su u posebnom položaju jer raspolažu manjim sredstvima i malobrojnijim ljudstvom. Zbog toga problemu zaštite podataka moraju da posvete posebnu pažnju. Ove aktivnosti treba sprovoditi pažljivo i sukcesivno, kako bi se snizili troškovi i greške svele na prihvatljiv minimum.

Posle detaljne analize tehnologije posla MSP, potencijalnih kriznih situacija, mogućih koncepcija i tehničkih rešenja, pre nabavke opreme potrebno je

ponovo sagledati da li su svi faktori razmotreni i uzeti u obzir. Posebnu pažnju treba posvetiti odgovoru na pitanje: Da li je moguće i koliko brzo je moguće oporaviti sistem, pa aplikacije i podatke staviti na raspolaganje korisnicima? Treba proveriti da li postoji pristup svim delovima sistema, svim komponentama koje su potencijalni izvori nastanka kriza, i da li se mogu brzo popraviti. Treba utvrditi algoritam po kome se pristupa oporavku palog servera. Takođe, zbog stalnih promena u poslovanju uvek treba imati u vidu i mogućnosti eventualnog proširenja sistema, promene pojedinih komponenata i povećanja broja korisnika.

Na kraju, treba imati u vidu i oblak-koncepciju, koja je sada relativno malo primenjena ali koja će se u narednih desetak godina najverovatnije nametnuti kao standardno rešenje za poslovanje MSP.

7. LITERATURA

1. McDermott, Adian. „A Small Business Approach to Computer Downtime“, www.user_groups.net
2. Available at www.virtual-strategy.com/Features/20100602-SteelEye.html
3. www.usanewsweek.com/news/Verizon-introduces-Cloud-Computing - CaaS -For-- SMB-1284495955
4. Otey M, „The Rise of Cloud Computing“, Windows IT Pro, InstantDoc ID#103674, April 2010
5. Reid A, Lorenz J, „Working at a Small/toMedium Business or ISP“, Cisco Press, ISBN-10: 1-58713-210-9, ISBN-13: 978-1-58713-210-0, April 2008
6. Čekerevac, Zoran. „Elektronsko poslovanje“. VPŠ Čačak. Čačak (2011)
7. Čekerevac, Z., Radović, D., Anđelić, S.:Data Protection in Small and Medium Sized Enterprises. Book of Abstracts. SMEPP_2011. Novi Pazar. April 2011.