

Da li ste spremni...



...da zbog **39 RSD dnevno**
izgubite Vaše podatke!!!

Da li neko trenutno u Vašoj firmi brine o kopiranju baza podataka?
Ako je odgovor NE, onda predlažemo da taj posao prepustite nama.

Šta dobijate?

Mi brinemo o dnevnim kopijama baza i garantujemo da nećete izgubiti podatke starije od 24h!

- ✓ Pet dnevnih kopija izabrane baze podataka za poslednja tri dana.
- ✓ Pet dnevnih kopija konfiguracione baze podataka za poslednja tri dana.
- ✓ Jedan dnevni test integriteta (ispravnosti) kopiranih baza.
- ✓ Dislociranje kopije baze sa Vašeg servera na naš cloud CBS server.
- ✓ Konstantni monitoring uspešnosti svih navedenih procedura.
- ✓ Kopija svih dostupnih baza (godina) na samom početku aktivacije usluge.
- ✓ Po ceni od 5 eura mesečno po bazi dobijate sigurnu kopiju.

Ukoliko nemate redovne kopije baza?

- 1 Povratak podataka sa servera gde je napravljena šteta od strane kriptolokera nije moguća i jedina opcija za nastavak poslovanja su kopije baza; a naše iskustvo govori da većina firmi neredovno pravi kopije baza, koje su samim tim beskorisne.
- 1 Cena radnog sata na serveru (kod različitih tipova gubljenja podataka) je 3,125.00 rsd i obično radovi traju 10-15h.
- 1 Oporavak oštećene baze podataka prosečno traje 3-5h i rezultati su neizvesni, a cena radnog sata je 4,375.00 rsd (samo za slučajeve gde nije došlo do napada na server od strane kriptolokera).



Cena može da varira i zavisi od veličine štete, pa je zbog toga nezahvalno raditi procenu trajanja radnih procesa na oporavku samih podataka.

U određenim slučajevima cena može da bude približno 500eur bez garancije za tačnost podataka u samoj bazi.

Mi smo tu da Vam pomognemo

CBS Tehnologija

Centralizovani backup sistem - tehnologija koja čuva vaše baze podataka daleko od napadača i čini Vaš biznis sigurnim!



Poštovani korisnici,

Poslednjih nekoliko godina najrasprostranjeniji tip malware-a je ransomware i njegove podvarijante kriptovirusi, koji su postali ogromna pretnja za Vaše baze podataka na serverima, a bez backup-a baza ni jedna firma više nije sigurna. Naše dugogodišnje iskustvo sa ovim tipom pretnji nam govori da su podjednako ugrožene i velike i male firme, i u većini slučajeva napadači ne biraju žrtve po obimu poslovanja i vrednosti firme.

Najpoznatiji tipovi anti virus (anti malware) zaštita nisu efikasni u ovim slučajevima jer postoji veliki broj Cripo Locker-a koji se menjaju na dnevnom nivou i postaju praktično neuhvatljivi za postojeće tipove antivirus zaštite.

Proboj (ulazak) kriptovirusa u vašu lokalu mrežu vrši se na dva načina:

- Preko "važnih" dokumenata i faktura koji su namenjeni i adresirani na Vašu firmu, a distribuiraju se preko programa za komunikaciju (Skype, Viber, WhatsApp i sl.), email-ovima i direktnim skidanjem fajlova sa interneta.
- Drugi način je direktan napad na Vaš server: preko programa za daljinsko upravljanje (slabe lozinke), usled propusta u operativnom sistemu od strane proizvođača, ili neažuriranog servera kojem nisu zakrpljene sve bezbednosne rupe.

Nakon proboja u većini slučajeva kriptovirus ostaje pritajen i čeka komandu napadača koji ne pokreće napad sve do trenutka dok ne uspe da priđe Vašim najbitnijim podacima, a to je upravo server i Vaše baze podataka. Dakle, napadač u većini slučajeva ne vrši proboj direktno na Vaš server, neko preko najslabije tačke u firmi a to je mreža klijent računara i radnika koji ne mogu ispravno prepoznati da je u toku napad. Preko lažnih linkova i dokumenata u kojima se nalaze izvršni programi (virusi) sa trenutno najopasnijim kontejnerima kodova unutar sebe napadač prodire u Vašu lokalnu mrežu.

Po ulasku na server, napadač obično započinje plansku proceduru napada neradnim danom, u večernjim satima kada je server najmanje opterećen, i kada nema nikoga prisutnog da primeti čudna dešavanja sa samim serverom (čudno ponašanje npr. opterećenje servera, neočekivanje promene podataka, realno može da uoči samo stručno lice ukoliko je prisutno u trenutku napada, pa i tada je mala verovatnoća da će uspeti na vreme da zaustavi kompletan napad). Kriptovanje (zaključavanje) baza se vrši trenutno tako da napadač svoj posao završava u veoma kratkom vremenskom roku, što mu je i cilj jer želi da ostane neopažen u vreme trajanja napada. Napadač na kraju ostavlja ucenu i instrukcije za plaćanje preko kriptovaluta koje mu pružaju sigurnost da će ostati neotkriven, uz uslov da će ključ za dekriptovanje (otključavanje) podataka i baza biti dostavljen po izvršenoj uplati.

Postavlja se pitanje da li napadaču treba verovati i izvršiti uplatu koja realno ne garantuje da će Vaši podaci biti otključani, a pristankom na ucenu postajete zanimljivi za sledeći napad. Naše dosadašnje iskustvo govori da ne treba pristati na ucenu i platiti traženu sumu.

Redovan backup baza je jedino rešenje za ovaj tip napada, ali samo ukoliko se baze dislociraju sa lokalnog servera na spoljne servere, koji zbog svoje tehnologije i procedure rada nude sigurno mesto za smeštanje Vaših baza.

Redovnim kopiranjem baza čuvate Vaše podatke i biznis!

Podržani tip čuvanja baza



1. Lokalno

- slab nivo zaštite -

U okviru samog servera na sistemskom disku i drugom hard disku ili partitiji.



2. Lokalno

- slab nivo zaštite -

Na eksternom memorijskom prostoru (HDD ili USB)



3. Cloud zaštita

- visok nivo zaštite -

Podrazumeva izmeštanje svih kopija baza sa lokalnog servera na udaljeni server 1 Click Soft-a sa maksimalnim sistemom zaštite. Ovaj tip čuvanja Vaših podataka daje potpunu sigurnost vašim bazama i biznisu!

Razlika između tipova čuvanja baza podataka

1. **Lokalno na serveru:** server je podložan hardverskim oštećenjima (nestanak struje, strujni udar, zamor elektronike, fizička oštećenja itd), softverska oštećenja (neispravno rukovanje operativnim sistemom i pripadajućim softverom, virusi, greške u programima i drugo).
2. **Lokalno na eksternim medijima:** osim hardverskih oštećenja, sve što je u dodiru sa ugroženim računarom i u najkraćem vremenskom periodu, postaje ugroženo i podložno gubitku podataka.
3. **Cloud zaštita:** najbolji vid zaštite koji zbog mogućnosti izmeštanja fajlova na udaljenu lokaciju više puta u toku dana van Vaše IT infrastrukture, pruža jedini siguran način za očuvanje podataka do trenutka pre samog napada.

Zašto baš Cloud zaštita

- ✓ Zaštita baza od mehaničkog kvara servera.
- ✓ Potpuna zaštita od kriptovirusa.
- ✓ Zaštita od slučajnog ili namernog brisanja baza.
- ✗ Mana, klijent koji ne shvata vrednost svojih podataka i biznisa.



Očekujemo Vaš poziv,
jer mi smo tu zbog Vas!



Kontaktirajte nas

Naš tim je dostupan za rad sa klijentima, putem navedenih kontakata.



Aleksandar

1 Click Soft



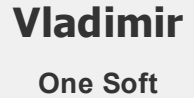
✉ aca@1clicksoft.rs

☎ 063 44 53 97



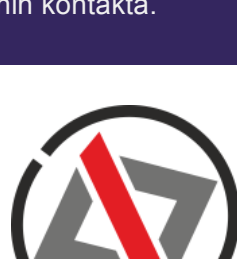
Vladimir

One Soft



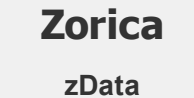
✉ vlada@1clicksoft.rs

☎ 063 658 219



Zorica

zData



✉ zoka@1clicksoft.rs

☎ 011 322 456 4

Radno vreme

Radno vreme:
Ponedeljak - Petak: 09:00 - 17:00h

Rad sa klijentima:
Ponedeljak - Četvrtak: 09:00 - 16:00h

Dostupni u kancelariji

Telefon: 011 322 456 4

Mobilni 1: 063 658 219
Mobilni 2: 063 44 53 97

Poslovno informacioni sistem Komercijalno poslovanje

Ovu e-mail poruku ste primili zato što ste korisnici 1 Click Soft, One Soft ili zData softverskih rešenja i usluga.