

# OUCH!

## U OVOM IZDANJU...

- Uvod
- Kako izabrati odgovarajući računarski oblak
- Kako osigurati bezbednost podataka

## Bezbedno korišćenje računarskog oblaka

### Uvod

„Oblak“ („The Cloud“), računarski oblak je moćna tehnologija koju kako pojedinci tako i organizacije sve više usvajaju i koriste. Računarski oblak za različite pojedince može da ima drugačije značenje, ali u principu podrazumeva korišćenje Internet servisa za skladištenje i upravljanje podacima. Prednost računarskog oblaka nije samo u jednostavnom pristupu i sinhronizaciji podataka između više uređaja ma gde se u svetu nalazili, nego

i u mogućnosti da jednostavno delite svoje informacija sa drugima. Razlog zbog koga se ovakav tip servisa nazva „Oblak“ je zato što često ne znamo gde su podaci fizički uskladišteni. Primeri korišćenja računarskog oblaka uključuju kreiranje dokumenata u okviru Google Docs-a, deljenje podataka pomoću Dropbox-a, postavljanje vlastitog servera na Amazon Cloud-u, ili skladištenje svoje muzike na Apple iCloud-u. Svi ovakvi Internet servisi obezbeđuju daleko veću produktivnost, ali takođe i podrazumevaju određeni rizik. U ovom izdanju objasnićemo kako da bezbedno koristite ovakve tipove servisa.

### Gost urednik

James and Kelli Tarala ([@isaudit](#) / [@kellitarala](#)) su glavni konsultanti u „Enclave Security“-ju i autori brojnih SANS kurseva, uključujući „SANS Audit 566: Implementing and Auditing the Twenty Critical Security Controls“ i „MGT 415: A Practical Introduction to Risk Assessments“.

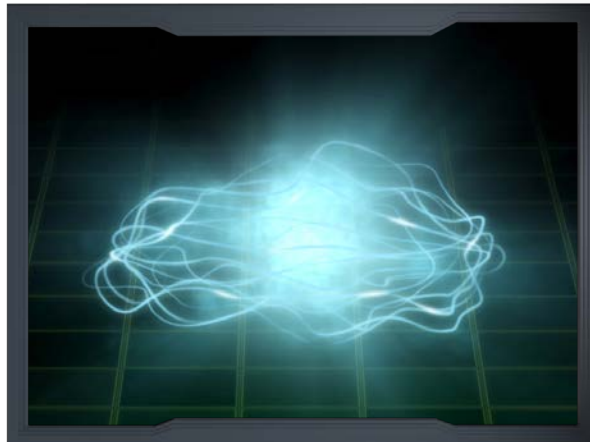
### Kako izabrati odgovarajući računarski oblak

Računarski oblak nije ni dobar ni loš, to je samo jedan od alata koje koristimo, bilo na poslu ili kod kuće. Međutim, kada koristite ovakav tip servisa, gde svoje privatne i lične podatke poveravate na čuvanje potpunim strancima, očekujete da vaši podaci budu i bezbedni i dostupni. Samim tim, želite da budete sigurni da ste napravili pravi izbor. U vezi mogućnosti korišćenja ovih servisa u poslovne svrhe, proverite sa vašim nadređenim ili IT podrškom. Ako vam je korišćenje dozvoljeno, proverite koje servise možete da koristite i upoznajte se sa odgovarajućom bezbednosnom politikom vaše organizacije i dozvoljenom načinu korišćenja. Ako imate na umu da koristite ovakve servise u privatne svrhe imajte na umu sledeće.

1. **Podrška:** Koliko je jednostavno dobiti pomoć ili odgovor na pitanje? Da li postoji telefon ili adresa el. pošte za kontakt? Da li postoje drugi oblici podrške, kao što su javni forumi ili često postavljena pitanja (FAQ)?

## Bezbedno korišćenje računarskog oblaka

2. **Jednostavnost:** Koliko je servis jednostavan za korišćenje? Što je servis složeniji za korišćenje, mogućnost greške ili slučajne kompromitacije informacija je veća. Uzmite u obzir servise koji su vam laki za razumevanje, konfiguraciju i korišćenje.
3. **Bezbednost:** Kako će se vaši podaci prenositi sa vašeg računara u računarski oblak, da li je veza obezbeđena enkripcijom? Kako su podaci uskladišteni, da li su enkriptovani, i ako jesu, ko može da ih dekriptuje?
4. **Uslovi korišćenja:** Nađite vremena da pregledate uslove korišćenja (obično su jednostavni za čitanje). Utvrdite ko može da pristupi vašim podacima i koja su vaša zakonska prava.



*Računarski oblak omogućava veću produktivnost i lakši pristup, ali budite veoma pažljivi kako skladištite i delite svoje podatke.*

## Kako osigurati bezbednost podataka

Kada ste odabrali odgovarajući računarski oblak, sledeće što je potrebno je da osigurate njegovo ispravno korišćenje. Često je za bezbednost podataka najbitniji sam način kako pristupate i delite podatke. Neki od koraka koje treba imati na umu su.

1. **Autentifikacija:** Za autentifikaciju na račun računarskog oblaka koristite jaku, jedinstvenu propusnu frazu. Koristite autentifikaciju iz dva koraka ako je podržana od strane servisa.
2. **Deljenje fajlova/foldera:** Računarski oblak omogućava jednostavno deljenje, poneka i suviše jednostavno. U najgorem slučaju, moguće je da svoje fajlove ili čak čitave foldere dostupne svim korisnicima Interneta. Najbolji način zaštite je da kao podrazumevano podešavanje ne delite svoje fajlove ni sa kim. Onda pristup dozvolite samo odgovarajućim osobama (ili grupama) odgovarajućim fajlovima ili folderima po osnovu „moraju da znaju“. Kada neko nema više potrebe za pristupom, uklonite mu odgovarajuća prava. Servis koji koristite treba da ima mogućnost da lako kontrolišete ko ima pristup vašim fajlovima i folderima.
3. **Deljenje fajlova/foldera korišćenjem veza („links“):** Jedna od zajedničkih osobina računarskih oblaka je mogućnost da kreirate mrežnu vezu („web link“) koji ukazuje na vaše fajlove ili foldere. Na taj način moguće je deliti svoje podatke tako što je dovoljno poslati samo „web link“. Međutim ovakav način je veoma nesiguran, pošto svako ko zna ili ima pristup „web link“ može da pristupi podacima. Ako „web link“ pošaljete

## Bezbedno korišćenje računarskog oblaka

nekoj osobi, ta osoba može da podeli isti „web link“ sa drugima ili se čak može naći u Internet pretraživačima. Ako delite svoje podatke korišćenjem „web link-a“, imajte na umu da ga deaktivirate kad više ne bude potrebno, ili ako je moguće, zaštitite ga lozinkom.

4. **Podešavanja:** Budite sigurni da ste razumeli podešavanja ponuđena od servisa koji koristite. Na primer, ako podelite svoje podatke sa nekim, da li ona/on može te vaše podatke da podeli sa drugima bez vašeg znanja?
5. **Antivirus:** Budite sigurni da ste instalirali najnoviju verziju antivirus program, sa najnovijim definicijama, na svim uređajima sa kojih pristupate ili delite svoje podatke. Ako je fajl koji delite inficiran, i drugi uređaji koji mu pristupaju mogu da se inficiraju.
6. **Rezervne kopije (backup):** Pored toga što servis koji koristite pravi rezervne kopije podataka, uzmite u obzir da i sami to činite. Ne samo da ste na taj način osigurani kao servis koji koristite prestane da funkcioniše, bude ugašen ili iz bilo kog razloga nedostupan, nego je i dosta lakše oporaviti velike količine podataka i lokalne rezervne kopije nego da ih „povlačite“ iz računarskog oblaka. Takođe, budite upoznati sa činjenicom koliko često servis koji koristite pravi rezervne kopije, da li omogućavaju oporavak ranijih verzija fajlova i koliko dugo čuvaju rezervne kopije?

## Saznaj Više

Prijavi se na OUCH! mesečni bilten bezbednosnih saveta za korisnike računara, pristupi prethodnim OUCH! izdanjima i saznaj više o SANS rešenjima u vezi svesnosti bezbednosti informacija na našoj internet prezentaciji

<http://www.securingthehuman.org/>

## Dodatne informacije

- Jake lozinke: <http://www.securingthehuman.org/ouch/2013#may2013>
- Menadžeri lozinki: <http://www.securingthehuman.org/ouch/2013#october2013>
- Rezervne kopije: <http://www.securingthehuman.org/ouch/2013#september2013>
- Bezbednosni termini: <http://www.securingthehuman.org/resources/security-terms>

OUCH! Objavljuje SANS Securing The Human program i distribuira se pod [Creative Commons BY-NC-ND 4.0 licencom](http://creativecommons.org/licenses/by-nc-nd/4.0/). Biltene je dozvoljeno distribuirati ili koristiti za svoj program unapređenja bezbednosne svesti uz uslov da sadržaj nije modifikovan. U vezi prevoda ili za dodatne informacije, kontaktiraj [ouch@securingthehuman.org](mailto:ouch@securingthehuman.org).

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis  
Preveo: Nenad Varinac



[securingthehuman.org/blog](http://securingthehuman.org/blog)



[/secrethehuman](https://www.facebook.com/secrethehuman)



[@secrethehuman](https://twitter.com/secrethehuman)



[securingthehuman.org/gplus](http://securingthehuman.org/gplus)