

OUCH!

U OVOM BROJU...

- Uvod
- Izbor Cloud provajdera
- Zaštita vaših podataka

Bezbedno korišćenje Cloud-a

Uvod

Računarski oblak („The Cloud“) može da označava različite stvari za različite ljude, ali pod pojmom Cloud obično se podrazumeva korišćenje usluga na Internetu za smeštaj i upravljanje vašim računarskim sistemima i/ili vašim podacima. Prednost Cloud-a je da možete lako da pristupate i sinhronizujete vaše podatke sa više uređaja bilo gde u svetu, i što takođe možete da podelite vaše informacije s kim god želite. Ove servise zovemo Cloud (računarski oblak) zato što često ne znate gde se vaši podaci fizički nalaze. Primeri Cloud usluga uključuju kreiranje dokumenata na Google Docs-u, deljenje podataka putem Dropbox-a, postavljanje vlastitog servera na Amazon Cloud-u, čuvanje podataka o kupcima na Salesforce-u ili arhiviranje vaše muzike ili slika na Apple iCloud-u. Ovi Internet servisi vas mogu učiniti daleko produktivnijim, ali oni sa sobom takođe donose i određene rizike. U ovom broju objašnjavamo kako da na bezbedan način iz Cloud rešenja izvučete najviše.

Gost urednik

Dave Shackelford ([@daveshackelford](https://twitter.com/daveshackelford)) je profesionalni konsultant, vlasnik kompanije Voodoo Security i autor brojnih SANS kurseva, uključujući i SANS Security 579: Virtualization and Private Cloud Security i Security 524: Cloud Security Fundamentals.

Izbor Cloud provajdera

Cloud nije ni dobar ni loš sam po sebi, to je alat za obavljanje poslova, kako na radnom mestu tako i kod kuće. Ipak, kada koristite ove servise vi poveravate vaše privatne podatke drugima na čuvanje i očekujete od njih da se staraju da vam podaci budu i zaštićeni i dostupni. Upravo zato, želite da budete sigurni da ste napravili ispravan izbor prilikom odabira Cloud provajdera. Ako planirate da koristite Cloud na poslu i za poslovne informacije obavezno prvo proverite politiku kompanije i konsultujte se sa vašim nadređenim da biste saznali da li vaša kompanija dozvoljava korišćenje Cloud servisa. Ukoliko vam je dozvoljeno da koristite Cloud, proverite koje servise možete da koristite i kakve su politike i pravila za njihovo korišćenje. Ako razmišljate o Cloud servisu za vaše privatne potrebe, razmotrite sledeće:

1. **Podrška** Koliko je jednostavno dobiti pomoć ili odgovor na postavljeno pitanje? Da li postoji adresa elektronske pošte koju možete kontaktirati, forum na kojem možete da postavljate pitanja ili lista najčešće postavljenih pitanja na njihovom veb sajtu?
2. **Jednostavnost** Koliko je lako korišćenje servisa? Što je servis komplikovaniji za korišćenje veća je verovatnoća da

Bezbedno korišćenje Cloud-a

ćete napraviti grešku i slučajno otkriti ili izgubiti svoje informacije. Izaberite Cloud provajdera čiji servis je lak za razumevanje, konfigurisanje i korišćenje.

3. **Bezbednost** Da li se prikupljaju podaci o vama samima i koji? Kako će se vaši podaci prenositi sa vašeg računara u Cloud i kako se čuvaju u Cloud-u, da li su kriptovani, i ako jesu, ko može da ih dekriptuje?
4. **Uslovi korišćenja:** Izdvojite malo vremena da proučite Uslove korišćenja (oni su često iznenađujuće jednostavni za čitanje). Proverite ko može da pristupa vašim podacima i koja su vaša zakonska prava, kao i obaveze u pogledu bezbednosti koje je preuzeo provajder ili se one zahtevaju od vas.

Zaštita vaših podataka

Kada ste odabrali provajdera Cloud servisa, sledeći korak je da se osigurate da vaše Cloud servise ispravno koristite. Način na koji pristupate i delite vaše podatke može često imati daleko veći uticaj na bezbednost vaših podataka nego bilo šta drugo. Neki od ključnih koraka koje možete preduzeti uključuju sledeće:

1. **Autentifikacija:** Koristite jake i jedinstvene propusne fraze da biste se autentifikovali na vaš Cloud nalog. Ako vaš Cloud provajder nudi dvofaktorsku autentifikaciju preporučujemo da je koristite. Ovo je jedan od najvažnijih koraka koje možete preduzeti kako biste zaštitili svoj nalog.
2. **Deljenje fajlova/direktorijuma:** Cloud čini da deljenje fajlova bude veoma jednostavno, ponekad i previše jednostavno. U najgorem slučaju, vi možete misliti da vaše fajlove delite sa određenom osobom, a u stvari ste greškom svoje fajlove ili čitave direktorijume učinili javno dostupnim čitavom Internetu. Najbolji način da zašтите sebe je da vam podrazumevano (default) podešavanje bude da ne delite nijedan od vaših fajlova sa bilo kim. Potom pristup određenim fajlovima ili direktorijumima dozvolite samo određenim osobama (ili grupama) po principu najmanje potrebnih prava (need-to-know basis). Kada nekome više nije potreban pristup vašim fajlovima, uklonite ta prava pristupa. Vaš Cloud provajder bi trebalo da omogući da na jednostavan način pratite ko ima pristup vašim fajlovima i direktorijumima.
3. **Deljenje fajlova/direktorijuma korišćenjem linkova:** Česta (uobičajena) funkcionalnost nekih Cloud servisa je mogućnost da se kreira veb link koji ukazuje na vaše fajlove ili direktorijume. Ova funkcionalnost vam omogućava da jednostavno delite ove fajlove s kim god želite tako što ćete samo proslediti veb link. Ipak, ovaj pristup sadrži vrlo malo bezbednosti u sebi, svako ko zna ovaj link može imati pristup vašim ličnim fajlovima ili direktorijumima. Ako pošaljete link samo jednoj osobi, ta osoba može da podeli taj link sa drugima ili on može da se pojavi u Internet pretraživačima.



Cloud može učiniti vaše informacije dostupnijim a vas same produktivnijim, ali budite veoma oprezni kako pristupate vašim informacijama i kako ih delite.

Bezbedno korišćenje Cloud-a

Ako delite vaše podatke korišćenjem linka, ukinite link onda kada vam on više nije potreban tako što ćete podesiti datum isteka ili ako je moguće, zaštitite link lozinkom.

- Podešavanje:** Dobro proučite bezbednosna podešavanja koja vam nudi Cloud provajder. Na primer, ako podelite direktorijum sa nekim, da li taj neko može vaše podatke da podeli s drugima bez vašeg znanja? Takođe da li postoji mogućnost da vidite ko je i kada pristupao sadržaju koji delite. Da li možete da ograničite deljenje tako da osobe s kojima delite fajlove imaju samo prava za čitanje (read only) umesto za čitanje i pisanje (read+write) koja drugima omogućavaju i da izmene vaše fajlove?
- Antivirus:** Postarajte se da najnovija verzija antivirusnog softvera bude instalirana na vašem računaru i na svakom drugom računaru koji koristite za deljenje vaših podataka. Ako se fajl koji delite zarazi malicioznom kodom i drugi računari koji pristupaju tom istom fajlu mogu takođe da se inficiraju.

Saznajte više

Prijavite se na OUCH! mesečni bilten za podizanje svesti o bezbednosti informacija namenjen svima, pročitajte prethodne brojeve OUCH!-a i saznajte više o SANS-ovim rešenjima za unapređenje svesti o bezbednosti informacija na našoj internet prezentaciji securingthehuman.sans.org/ouch/archives.

Verzija na srpskom

Telekom Srbija kao društveno odgovorna telekomunikaciona kompanija pomaže prevođenje i distribuciju ovog biltena kako bi se unapredila svest korisnika informaciono-komunikacionih tehnologija o bezbednosti informacija.

Dodatne informacije

Verifikacija iz dva koraka:	https://securingthehuman.sans.org/ouch/2015#september2015
Propusne fraze:	https://securingthehuman.sans.org/ouch/2015#april2015
Menadžeri lozinki:	https://securingthehuman.sans.org/ouch/2015#october2015
Šta je malver:	https://securingthehuman.sans.org/ouch/2016#march2016
SEC524: Cloud Security Fundamentals:	https://sans.org/sec524

OUCH! bilten objavljuje SANS Securing The Human program i distribuira se pod [Creative Commons BY-NC-ND 4.0 licencom](https://creativecommons.org/licenses/by-nc-nd/4.0/). Biltene je dozvoljeno distribuirati ili koristiti za svoj program unapređenja svesti o bezbednosti informacija pod uslovom da se sadržaj ne modifikuje. Za pitanja u vezi prevoda ili za dodatne informacije, kontaktirajte ouch@securingthehuman.org.

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis Cheryl Conley
Preveli: Dragan Ristić i Gordana Živanović



securingthehuman.sans.org/blog



[/securethehuman](https://securethehuman)



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



securingthehuman.sans.org/gplus