OUCH! Avgust 2021

SANS SECURITY AWARENESS

Vaš mesečni bilten za podizanje svesti o bezbednosti informacija

Bezbedno korišćenje Cloud-a

Uvod

Bez ikakve sumnje ste već čuli za pojam klaud, računarstvo u oblaku (eng. Cloud computing). Ovaj pojam se odnosi na korišćenje usluga za smeštaj i upravljanje podacima koje nude brojni pružaoci usluga na internetu. Primeri uključuju kreiranje dokumenata na Google Docs-u, pristup mejlu putem Microsoft O365 usluga, deljenje podataka putem Dropbox-a, ili čuvanje vaših fotografija na Apple iCloud-u. Dok pristupate i sinhronizujete vaše podatke sa različitih uređaja bilo gde u svetu i razmenjujete ih s kim god želite, često ne znate i ne možete da kontrolišete gde se vaši podaci fizički nalaze.

Izbor pružaoca Cloud usluga

Sami po sebi, Cloud servisi nisu ni dobri ni loši. Oni jednostavno predstavljaju alate za obavljanje poslova. Ipak, kada koristite ove servise vi u suštini predajete vaše privatne podatke strancima, očekujući od njih da se staraju o njihovoj bezbednosti i dostupnosti. Upravo zato želite da budete sigurni da ste napravili mudar izbor pružaoca Cloud usluga. Za poslovne informacije obavezno se prvo konsultujte sa vašim nadređenim da biste saznali da li vam je dozvoljeno da koristite Cloud servise, kao i koji su to servisi dozvoljeni. Ako razmatrate korišćenje Cloud usluga za vaše privatne potrebe, razmotrite sledeće:

1. **Poverenje:** Možete li da verujete pružaocu Cloud usluga? Da li se radi o kompaniji koja je u javnosti dobro poznata i ima milione korisnika, ili je u pitanju mala, nepoznata kompanija sa sedištem u zemlji za koju nikada niste čuli?
2. **Podrška**: Koliko je jednostavno dobiti pomoć ili odgovor na postavljeno pitanje? Postoji li broj telefona koji možete pozvati ili adresa elektronske pošte na koju se možete obratiti? Postoje li i druge vrste podrške, poput javno dostupnog foruma ili liste najčešće postavljenih pitanja na njihovom veb sajtu?
3. **Jednostavnost**: Da li se usluga koristi na jednostavan način? Što je usluga komplikovanija za korišćenje veća je verovatnoća da ćete napraviti grešku i slučajno otkriti ili izgubiti vaše informacije. Izaberite pružaoca Cloud usluga čiji servis je lak za razumevanje, konfigurisanje i korišćenje.
4. **Bezbednost**: Kako će se vaši podaci prenositi od vašeg računara do Cloud usluge? Da li je konekcija sa Cloud-om zaštićena enkripcijom? Kako se vaši podaci čuvaju? Da li su enkriptovani, i ako jesu, ko sve može da ih dekriptuje? Dok migrirate podatke, ne zaboravite da je bezbednost zajednička odgovornost vas i provajdera.

5. **Kompatibilnost:** Da li pružalac usluga podržava sve uređaje i operativne sisteme koje koristite ili planirate da koristite?
6. Uslovi korišćenja: Izdvojte malo vremena da proučite Uslove korišćenja (oni su često iznenađujuće jednostavni za čitanje).Prema zakonima koje zemlje je pružalac usluga u obavezi da postupa? Obratite posebnu pažnju na prava koja ustupate vašem pružaocu usluga.

Zaštita vaših podataka

Sledeći korak je da osigurate da Cloud servise koristite na ispravan način. Način na koji pristupate i delite vaše podatke često može 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, jedinstvene lozinke da zaštitite vaš nalog na Cloud-u. Ako vaš pružalac Cloud usluga podržava dvofaktorsku autentifikaciju toplo preporučujemo da je koristite.
2. **Deljenje fajlova/direktorijuma**: Pružaoci Cloud usluga omogućavaju da razmena podataka bude veoma jednostavna, ponekad i previše. Zbog toga se može veoma lako dogoditi da informacije slučajno učinite javno dostupnim. Zaštitite se tako što ćete samo određenim ljudima (ili grupama ljudi) dozvoliti pristup određenim fajlovima ili direktorijumima. Kad nekome pristup više nije potreban, ukinite ga. Vaš pružalac Cloud usluga bi trebalo da omogući da na jednostavan način pratite ko ima pristup vašim fajlovima i direktorijumima.
3. **Podešavanja**: Dobro proučite bezbednosna podešavanja koja vam pružalac Cloud usluga nudi. Na primer, ako podelite fotografije, fajlove ili direktorijum sa nekim, da li taj neko može te vaše podatke da podeli s drugima bez vašeg znanja?
4. **Obnavljanje**: Ne zaboravite da na vreme obnovite pretplatu jer bi se u suprotnom moglo dogoditi da izgubite pristup svojim podacima.

Gost urednik

Tameika Rid (@womeninlinux) je osnivateljka organizacije Women in Linux. Začetnica je inicijativa usmerenih na istraživanje karijere u domenu infrastrukture, sajber bezbednosti, DevSecOps-a i liderstva. Organizatorka je redovnih nedeljnih okupljanja na kojima se razmatraju teme u rasponu od infrastrukture do blokčejna. Govorila je na konferencijama OSCon, LISA, Seagl i HashiConf EU.

Dodatni materijal

Socijalni inženjering: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Napravite lozinku na jednostavan način: https://www.sans.org/newsletters/ouch/making-passwords-simple/
Menadžeri lozinki: https://www.sans.org/newsletters/ouch/password-managers/
Moć ažuriranja:https://www.sans.org/newsletters/ouch/the-power-of-updating/

Preveli za zajednicu: Dragan Ristić i Gordana Živanović