softconsulting

**Autor: Lejla Softić, dipl.oec.**[1]

# Sigurnosni aspekti računovodstva 'u oblaku'

„Jedinu pravu sigurnost u današnjem svijetu čovjeku mogu pružiti znanje, iskustvo i sposobnost."
- Henry Ford

Sigurnost i zaštita finansijskih podataka tema je koja će uvijek biti aktuelna, bez obzira koji softver koristite za izvršavanje operativih aktivnosti u računovodstvu i finansijskom upravljanju. Svaki korisnik, a naročito međunarodna grupacija[2], prije nego se opredijeli za primjenu računovodstva 'u oblaku' želi znati da su finansijski podaci adekvatno zaštićeni i dostupni, u skladu sa dodijeljenim ovlastima (CFO, računovođa i drugi korisnici u IT sistemu).

**Kontrola pristupa**[3] je način ograničavanja pristupa sistema fizičkih ili virtualnih resura. U računarstvu, kontrola pristupa je proces kojim se korisnicima omogućava pristup i određene privilegije u sistemima, resursima ili informacijama. Sistemi za kontrolu pristupa služe za dodjeljivanje prava ko, kada i gdje može da pristupi štićenom prostoru. Kontrolom pristupa se reguliše ulazak u i/ili izalak iz štićenog prostora. U računarskoj bezbjednosti, kontrola pristupa uključuje ovlašćenje, autorizaciju i odobrenje za pristup resursima na računaru.


Kod smještanja podataka 'u oblak' korisniku nije bitno gdje se ti podaci nalaze sve dok se poštuje:

- privatnost podataka,
- zaštita od neovlaštenog pristupa,
- integritet podataka,
- dostupnost,
- brz pristup podacima,
- ugovorni odnos koji će zakonski regulirati prava i obaveze i korisnika i pružatelja usluge.

Smještanjem finansijskih podataka 'u oblak' odnosno korištenjem alata računovodstva 'u oblaku' međunarodna grupacija može efikasnije pristupati i koristiti informacije u preduzećima kćerkama, bez potrebe za njihovim direktnim angažiranjem pri razmjeni podataka unutar grupacije. Stoga su sigurnosni aspekti primjene računovodstva 'u oblaku', za međunardne grupacije, od posebnog značaja. Svaki neovlašteni pristup podacima odnosno tzv. hakiranje[4] cjelokupnog računovodstvenog sistema za međunarodnu grupaciju može biti potencijalni rizik sa nesagledivim posljedicama. Znajući to, međunarodna grupacija treba da bude adekvatno pripremljena za ovakav način upravljanja rizicima odnosno ne treba da odustane od primjene prednosti računovodstva 'u oblaku' i treba pravovremeno da kreira odgovarajuće sisteme zaštite finansijskih podataka i računovodstvenog (i IT) sistema kao cjeline.

---

1 SoftConsulting s.p. Tuzla,Trg slobode 16 ( BIT Centar), 750000 Tuzla, e-mail: lejla.softic@savjetnik.ba
Izvor za sliku: https://pixabay.com/en/sure-castle-privacy-policy-security-1435364/
2 Op.a. Sve navedeno u tekstu odnosi se i na MSP kao korisnike, a ne samo na međunarodne grupacije.
3 Izvor: https://sr.m.wikipedia.org/sr-el/%D0%9A%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D0%B0_%D0%BF%D1%80%D0%B8%D1%81%D1%82%D1%83%D0%BF%D0%B0
4 Hakeri su osobe koji vole kroz pozitivnu znatiželju istraživati granice onoga što je moguće, to često uključuje prepravljanje postojećih hardverskih i softverskih rješenja kako bi dobila novu funkciju ili otključala neku skrivenu. Izvor: https://hr.wikipedia.org/wiki/Haker

Adekvatan sistem zaštite finansijskih podataka 'u oblaku' započinje izborom odgovarajućih pružatelja usluga računovodstva 'u oblaku', koji ima posvećene stručnjake čiji je jedini zadatak da prate stanje u mreži odnosno da aktivno djeluju ukoliko se detektuje pokušaj neovlašćenog pristupa. **Izbor pružatelja usluga računovodstva 'u oblaku' je stvar povjerenja**. To povjerenje se gradi i to ne samo na osnovu suvremene tehnologije koja se koristi, već i primjenjenog sistema bezbjednosti i ljudi koji su odgovorni za bezbjednost odnosno sigurnost finansijskih podataka. Nadalje, pri izboru odgovarajućeg pružatelja usluga računovodstva 'u oblaku' bitno je prikupiti informacije o kontrolama pristupa, praksi za procjenu ranjivosti i kontrolama za upravljanje zakrpama i konfiguracijom, a kako bi se utvrdilo da li se adekvatno zaštićuje računovodstveni sistem odnosno finansijski podaci u njemu.

Dijeljenje važnih podataka sa pružateljem usluga računovodstva 'u oblaku' uključuje prijenos znatne količine organizacijinih kontrola nad sigurnosti podataka pružatelju usluga. Zato je bitno da pružatelj usluga razumije potrebe privatnosti i sigurnosti podataka za konkretnu međunarodnu grupaciju. Također, bitno je i da je pružatelj usluga upoznat sa pravilima o sigurnosti i privatnosti podataka koja primjenjuje po vlastitoj nadležnosti.

Veoma važno je znati da su pružatelji usluga računovodstva 'u oblaku' odgovorni za zaštitu podatka koje pohranjuju odnosno za sigurnost infrastrukture koju su ponudili korisnima, ali da je za sigurnost aplikacija i servisa odgovornost na krajnjim korisnicima. Stoga što veliki dio odgovornosti ostaje i na korisnicima međunarodna grupacija treba znati da je za većinu sigurnosnih propusta odgovorna ljudska greška, i to zbog neznanja i/ili nepažnje. Upravo zato je educiranje zaposlenika iznimno važno, gdje svi zaposlenici koji imaju pristup uslugama računovodstva 'u oblaku' moraju znati kako rukovati (finansijskim) podacima na siguran način, te kako spriječiti njihovu eventualnu zloupotrebu.

Kod sigurnosti, prevencija je bolja od terapije. Zato je važno primjeniti jednostavne i učinkovite mjere zaštite. Anti-virusni softver je obavezan. Odabir pametne lozinke je nužan, a lozinke treba i često mijenjati. Uz to, nužno je redovito raditi i kopije svih važnih podataka. Softver treba stalno ažurirati. Mrežu treba zaštiti u cijelosti, a ne samo neke uređaje.

**Zaključak**

Analiza sigurnosnih aspekata primjene računovodstva 'u oblaku' ne razlikuju se mnogo u odnosu na analizu bilo kojeg drugog aspekta, pri finansijskom upravljanju, u međunarodnoj grupaciji. Pri finansijskom upravljanju od posebnog značaja je kreirati i primjeniti politiku sigurnosti i zaštite povjerljivih i finansijskih podataka, kao dio ukupne finansijske politike međunarodne grupacije.

Dakle, zaštita finansijskih podataka 'u oblaku' nije samo stvar tehnologije. Kako bi obezbjedila odgovarajućuju zaštitu finansijskih podataka 'u oblaku' međunarodna grupacija treba da implementira određena pravila, kontrolu i sisteme koji ih obrađuju i čuvaju, što se postiže uspješnom implementacijom konkretne politike bezbjednosti, standarda, smjernica i procedura, pri čemu:

- **Politika** označava sve poslovne informacije koje moraju biti adekvatno zaštićene kada se prenose ili skladište.
- **Standard** za upravljanje informacijama zahtijeva da sve osjetljive informacije budu kriptovane korišćenjem određenog tipa kriptografije i da se svi prijenosi podataka bilježe (loguju).
- **Smjernice** objašnjavaju najbolju praksu za bilježenje prijenosa osjetljivih informacija i daju šeme za bilježenje prijenosa i rukovanje osjetljivim informacijama.
- **Procedure** daju postupne instrukcije kako da se izvrši kriptovanje pri prijenosu podataka i kako da se osigura usklađenost sa politikom, standardima i smjernicama.