Awareness raising campaign for SMEs

Pet koraka do sigurnog Cloud okruženja

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S RIGHTS, EQUALITY AND CITIZENSHIP 2014-2019 PROGRAMME UNDER GRANT AGREEMENT N°874524.

Okruženja temeljena na Cloud-u nude mnoge prednosti organizacijama. Međutim, ona također uvode niz tehničkih sigurnosnih rizika kojih bi organizacije trebale biti svjesne kao što su:

 povrede podataka

 Hakiranje računa

 Neovlašteni pristup osobnim podacima

Organizacije bi trebale odrediti i implementirati dokumentiranu politiku i primijeniti odgovarajuće tehničke sigurnosne i organizacijske mjere za osiguranje svojih okruženja temeljenih na Cloudu. Ako organizacije ne provedu takve kontrole, mogu povećati rizik od povrede osobnih podataka.

Organizacije bi takve tehničke sigurnosne i organizacijske mjere trebale primjenjivati na slojevit način koji se sastoji od sljedećih elemenata:

 Kontrole pristupa

 Vatrozid

 Antivirus

 Obuka osoblja

 Razvoj internih procedura

Slojeviti pristup sigurnosti temeljenoj na Cloudu ublažava rizik od neuspjeha jedne sigurnosne mjere, što može rezultirati povredom osobnih podataka.

Mnogi pružatelji usluga temeljenih na Cloudu, kao što su Microsoftov Office 365 i Googleov G-suite, pružaju napredne postavke i rješenja koja mogu pomoći organizacijama da na odgovarajući način osiguraju korištenje usluga temeljenih na Cloudu. Ti pružatelji usluga u većini slučajeva također nude smjernice za najbolju praksu kako bi pomogli organizacijama u osiguravanju svojih okruženja temeljenih na Cloudu.

Dodatne informacije, savjete i najbolju praksu u vezi sa sigurnošću okruženja temeljenih na Cloudu također pružaju agencije kao što je Agencija Europske unije za mrežnu i informacijsku sigurnost (“ENISA”) i Nacionalni institut za standarde i tehnologiju sa sjedištem u SAD-u (“NIST”).

Sljedeće smjernice ilustriraju pet ključnih načina na koje organizacije mogu osigurati svoja okruženja temeljena na Cloudu kako bi umanjili rizik od povrede osobnih podataka.

1. Kontrola pristupa i autentifikacija

Organizacije bi trebale implementirati **politike jakih zaporki** kako bi osigurale da korisnici koji pristupaju osobnim podacima unutar okruženja temeljenih na Cloudu to čine na siguran način.

Organizacije bi trebale implementirati **dvofaktorsku autentifikaciju**. **Dvofaktorska provjera autentičnosti** učinkovit je način za daljnje poboljšanje sigurnosti u Cloudu i dostupna je od većine pružatelja usluga u Cloudu.

Organizacije bi trebale biti svjesne i **dokumentirati privilegije pristupa korisnika** unutar svojih okruženja temeljenih na Cloudu. Kontrola pristupa korisnika posebno je važna kada se koriste grupni poštanski sandučići ili dijeljene mape. Organizacije bi također trebale dokumentirati specifične zahtjeve pristupa svakog korisnika i osigurati da su oni podržani odgovarajućim procesom kontrole promjena.

Sigurnosne mjere koje primjenjuje organizacija moraju biti podržane **redovitim pregledima** pristupa korisnika kako bi se osiguralo da je sav ovlašteni pristup osobnim podacima strogo nužan i opravdan za obavljanje određene funkcije.

2. Pregledajte zadane sigurnosne postavke

Organizacije se **ne bi trebale oslanjati** na zadane sigurnosne postavke pružatelja usluga u Cloudu. Organizacije bi trebale pregledati sigurnosne značajke temeljene na Cloudu dostupne od pružatelja usluga temeljenih na Cloudu kako bi osigurale da se primjenjuju na odgovarajući način i na slojevit način. Primjeri sigurnosnih postavki i kontrola koje pružaju pružatelji usluga u Cloudu često uključuju:

- Centralizirane administrativne alate
- Upravljanje mobilnim uređajima
- Višefaktorska autentifikacija
- Upozorenja za prijavu
- Enkripcija tijekom slanja i primanja poruke
- Enkripcija sadržaja poruke
- Praćenje aktivnosti računa i upozorenja
- Sprečavanje gubitka podataka
- Zaštita od zlonamjernog softvera
- Zaštita od neželjene pošte i lažiranja
- Zaštita od krađe identiteta

Organizacije bi također trebale biti svjesne da usluge temeljene na Cloudu mogu biti javno dostupne i organizacije bi trebale pregledati i implementirati odgovarajuće sigurnosne postavke kako bi osigurale **daljinski pristup**.

3. Potražite jamstva od svog pružatelja ICT usluga

Organizacije mogu **koristiti vanjske pružatelje ICT (Information and Communication Technology) usluga** za implementaciju svojih okruženja temeljenih na Cloudu. Od vitalnog je značaja tijekom takvih angažmana da organizacije traže **formalna jamstva** od svog pružatelja ICT usluga da provedene sigurnosne kontrole ispunjavaju specifične sigurnosne zahtjeve organizacije i štite osobne podatke organizacije.

Organizacije bi se trebale **proaktivno angažirati i provoditi redovite sigurnosne preglede** sa svojim pružateljima ICT usluga kako bi osigurale da su postojeće sigurnosne kontrole ažurne i učinkovite u zaštiti organizacije u okruženju prijetnji koje se neprestano razvija.

4. Jasna pravila i obuka osoblja

Organizacije bi trebale **osigurati da osoblje dobije odgovarajuću obuku** o napadima socijalnog inženjeringa, phishing napadima i praksama sigurnosnih prijetnji. Takva obuka treba biti podržana **programima osvježenja znanja/programima podizanja svijesti** kako bi se ublažio rizik koji predstavlja okruženje prijetnji koje se neprestano razvija.

Organizacije bi trebale imati **jasne politike** koje se odnose na korištenje i sigurnost usluga temeljenih na Cloudu, posebno kada se tim uslugama pristupa izvan korporativne mreže organizacije prema pravilima "*Donesi svoj vlastiti uređaj* " ("BYOD").

Organizacije bi trebale imati jasnu politiku **zadržavanja podataka** i provoditi **redovite preglede** kako bi osigurale da se osobni podaci ne zadržavaju dulje nego što je potrebno ili kada je prestala izvorna svrha upotrebe osobnih podataka.

5. Upoznajte svoje podatke i zaštitite ih

Organizacije bi trebale **razumjeti i pratiti vrste podataka** koji se pohranjuju u njihovim okruženjima temeljenim na Cloudu. Poznavanje vrsta podataka pohranjenih u Cloudu omogućuje organizaciji da osigura primjenu odgovarajuće sigurnosti i kontrole pristupa za zaštitu podataka.

Organizacije bi trebale koristiti **metode klasifikacije podataka** kako bi identificirale podatke koje pohranjuju i obrađuju unutar okruženja temeljenih na Cloudu. Proces klasifikacije podataka omogućuje organizaciji da kategorizira svoje pohranjene podatke kako bi odredila odgovarajuće sigurnosne kontrole.

Organizacije bi trebale **pažljivo procijeniti dobavljače temeljene** na Cloudu na temelju sigurnosnih značajki koje nude i na koji način ispunjavaju svoje organizacijske zahtjeve.

Tko ima pristup vašim podacima, kako je osiguran, koliko često se podaci sigurnosno kopiraju i je li okruženje temeljeno na Cloudu usklađeno s vašim organizacijskim politikama, vitalna su pitanja koja treba postaviti i vašem pružatelju usluga u Cloudu i/ili ICT pružatelju usluga zaduženom za implementaciju vašeg okruženja.

Primjena odgovarajućih sigurnosnih mjera **nije jednokratna vježba.** Sigurnosne postavke temeljene na Cloudu treba **redovito pregledavati** kako bi se osiguralo da su i dalje prikladne i ažurne.