OUCH! 2021. gada

OUCH!

SANS SECURITY AWARENESS

Ikmēneša informācijas drošības izdevums tev

Droša mākoņpakalpojumu lietošana

Pārskats

Iespējams, esi jau iepriekš dzirdējis par “mākoņa" pakalpojumiem. Tā ir pakalpojuma ņemšana interneta vidē, nododot savus datus apstrādei un uzglabāšanai. Kā piemērus var minēt dokumentu veidošanu Google Docs, piekļūšanu e-pastam Microsoft O365, dalīšanos ar datnēm, izmantojot Dropbox vai attēlu uzglabāšanu Apple iCloud. Piekļūstot un sinhronizējot datus no dažādām ierīcēm jebkurā pasaules nostūrī, un daloties ar informāciju ar jebkuru cilvēku, bieži nezini un nevari kontrolēt, kur fiziski tiek uzglabāti Tavi dati.

Mākoņpakalpojuma sniedzēja izvēlēšanās

Mākoņpakalpojumi nav nedz labi, nedz ļauni. Tas ir veids, kā kaut ko paveikt. Taču, izmantojot šos pakalpojumus, būtībā Tu nodod savus privātos datus svešiniekiem, sagaidot no viņiem, ka tie būs gan drošībā, gan pieejami. Līdz ar to Tev jābūt drošam, ka savu pakalpojuma sniedzēju izvēlies gudri. Attiecībā uz informāciju, kas saistīta ar darba jautājumiem, pavaicā savam vadītājam, vai drīksti izmantot mākoņpakalpojumus, un kurus tieši. Ja apdomā mākoņpakalpojumu izmantošanu privātām vajadzībām, padomā par:

1. **Uzticamību:** Vai vari uzticēties mākoņpakalpojumu sniedzējam? Vai tas ir plaši pazīstams, publisks uzņēmums, kura pakalpojumus jau izmanto miljoniem cilvēku, vai arī tā ir maza, nezināma kompānija, kas bāzēta valstī, par kuru nekad neesi dzirdējis?
2. **Atbalsts**: Cik viegli saņemt atbalstu kā pakalpojumu lietotājam un saņemt atbildes uz jautājumiem? Vai ir norādīts tālruņa numurs, uz kuru zvanīt vai e-pasta adrese? Vai pieejamas atbalsta opcijas, piemēram, biežāk uzdoto jautājumu sadaļa uzņēmuma vietnē?
3. **Vienkāršība**: Cik viegli izmantot pakalpojumus? Jo sarežģītāka ir pakalpojumu izmantošana, jo lielāka varbūtība, ka pieļausi kļūdas un nejauši atklāsi savu informāciju citiem vai pazaudēsi to. Izmanto mākoņpakalpojumus, kuri Tev šķiet viegli saprotami, pielāgojami un lietojami.
4. **Drošība**: Kā dati no Tava datora nokļūs pie mākoņpakalpojumu sniedzēja? Vai savienojums ir nodrošināts ar šifru? Kā Tavi dati tiek uzglabāti? Vai tie ir šifrēti, un, ja ir, kurš tos var atšifrēt? Migrējot datus, atceries, ka drošība ir dalīta atbildība starp Tevi un pakalpojumu sniedzēju.
5. **Saderība:** Vai šis pakalpojumu sniedzējs atbalsta visa veida ierīces un operētājsistēmas, kuras Tu lieto vai plāno lietot?

6. **Pakalpojumu noteikumi**: Velti laiku pakalpojumu noteikumu izlasīšanai (bieži vien tie ir pārsteidzoši viegli lasāmi). Saskaņā ar kuras valsts likumiem darbojas pakalpojumu sniedzējs? Īpašu uzmanību pievērs tiesībām, kuras nodod savam pakalpojumu sniedzējam.

Datu aizsargāšana

Nākamais solis ir pārliecināties, ka mākoņpakalpojumu izmanto pareizi. Tam, kā piekļūsti un dalies ar saviem datiem, bieži var būt daudz lielāka ietekme uz Tavu datu drošību, nekā jebkam citam. Dažas svarīgākās lietas, ko ņemt vērā:

1. **Autentifikācija**: Lai aizsargātu savu mākoņa lietotāja profilu, izmanto spēcīgu, unikālu paroli. Ja Tavs pakalpojumu sniedzējs piedāvā divu vai vairāku faktoru autentifikāciju, iesakām to izmantot.
2. **Dalīšanās ar datnēm/mapēm**: Mākoņpakalpojumu sniedzēji cenšas piedāvāt vienkāršu dalīšanos ar datiem. Reizēm pārāk vienkāršu. Var būt ļoti viegli nejauši dalīties ar savu informāciju publiskajā telpā. Aizsargā sevi, ļaujot tikai konkrētiem cilvēkiem (vai cilvēku grupām) piekļūt konkrētām datnēm vai mapēm. Kad kādam vairs nav vajadzīga piekļuve, noņem to. Tavam mākoņpakalpojumu sniedzējam vajadzētu nodrošināt Tev iespēju viegli sekot līdzi tam, kurš var piekļūt Tavām datnēm un mapēm.
3. **Iestatījumi**: Tev jāizprot mākoņpakalpojumu sniedzēja piedāvātie drošības iestatījumi. Piemēram, ja dalies ar attēliem, datnēm vai mapēm ar kādu citu, vai šī persona ar šiem datiem var dalīties tālāk, Tev to nezinot?
4. **Atjaunini**: Neaizmirsti atjaunināt abonementu, citādi vari zaudēt piekļuvi saviem datiem.

Viesredaktors

Tamika Rīda (@womeninlinux), “Women in Linux” dibinātāja. Viņa vada iniciatīvas, kas koncentrējas uz infrastruktūras, kiberdrošības, programmatūras ātrās piegādes (DevSecOps) un vadības karjeras iespēju izpēti. Viņa ir arī iknedēļas sarunu vadītāja, kur tiek pārrunāti dažādi jautājumi sākot no infrastruktūras līdz blokķēdēm. Viņa runājusi arī OSCon, LISA, Seagl un HashiConf EU konferencēs.

Resursi

Sociālās inženierijas uzbrukumi: https://www.sans.org/newsletters/ouch/messaging-smishing-attacks
Vienkāršu paroļu veidošana: https://www.sans.org/newsletters/ouch/making-passwords-simple
Paroļu pārvaldnieki: https://www.sans.org/newsletters/ouch/password-managers/
Atjauninājumu nozīme: https://www.sans.org/newsletters/ouch/the-power-of-updating

Tulkojums: CERT.LV