Mėnesinis informacinio saugumo naujienlaiškis kompiuterių naudotojams

OUCH!

ŠIAME LEIDINYJE…

Kaip saugiai naudoti debesiją?

Apžvalga

Įvairiems žmonėms terminas „debesija“ gali reikšti skirtingus dalykus, tačiau įprastai tai reiškia interneto paslaugų teikėjo pasirinkimą, siekiant internete laikyti ir tvarkyti duomenis apdorojančias sistemas bei/arba savo duomenis. Debesijos pranašumas yra tas, kad prie šių duomenų labai lengva prisijungti ir juos sinchronizuoti iš daugybės, bet kurioje pasaulio vietoje esančių, įrenginių. Be to, savo informacija galite dalytis su kuo tik pageidaujate. Šios paslaugos vadinamos „debesija“, kadangi dažnai nežinoma, kur duomenys yra laikomi fiziškai. Debesijos pavyzdžiais gali būti dokumentų kūrimas „Google Docs“ sistemoje, dalijimasis failais naudojant „Dropbox“, asmeninio serverio nustatymas „Amazon Cloud“, pirkėjų duomenų laikymas „Salesforce“ ar muzikos ir nuotraukų archyvavimas „Apple“ priklausančioje „iCloud“ sistemoje. Šios internetinės paslaugos gali ne tik padėti tapti produktyvesniais, bet ir pasižymi savitais pavojais. Šiame naujienlaiškyje apžvelgsime, kaip galite saugiai pasinaudoti didžiausiais debesijos teikiamais privalumais.

Kviestinė redaktorė

Dave Shackleford (**@daveshackleford**) yra įmonės „Voodoo Security“ įkūrėjas, taip pat profesionalus konsultantas ir daugybės SANS instituto kursų mokomosios medžiagos autorius, įskaitant tokius saugumo kursus kaip SEC579 „Virtualizacija ir privačios debesijos saugumas“ bei SEC524 „Debesijos saugumo pagrindai“.

Kaip pasirinkti debesijos paslaugų teikėją?

Debesija – tai tiesiog įprasta priemonė, padedanti atlikti tiek namų, tiek darbo užduotis. Be abejonės, naudodamiesi šiomis paslaugomis, kurių metu perduodate savo asmeninius duomenis kitiems, jūs tikitės, kad jie bus ne tik saugiai laikomi, bet ir to, jog prie jų bus lengva prisijungti. Todėl vertėtų įsitikinti, kad išmintingai pasirinkote savo debesijos paslaugų teikėją. Kalbant apie darbo kompiuterius ar su darbu susijusią informaciją, apie tai turėtumėte pasikalbėti su savo prižiūrėtoju ir pasidomėti, ar jūsų įmonėje leidžiama naudotis debesijos paslaugomis. Jei jums leidžiama jomis naudotis, tada turite pasiteirauti, kokiomis debesijos paslaugomis galite naudotis ir kokios taisyklės yra taikomos jų naudojimui. Jei svarstote pasinaudoti debesijos paslaugomis savo asmeninėms reikmėms, apsvarstykite toliau pateiktus klausimus:

1. **Pagalba**. Ar jums lengvai suteikiama pagalba arba atsakoma į jūsų klausimus? Ar debesijos paslaugų svetainėje yra nurodytas el. pašto adresas, kuriuo, prireikus, galima susisiekti? Ar joje yra vieši forumai, kuriuose galite aptarti

Kaip saugiai naudoti debesiją?

jus dominančius klausimus? Ar yra dažnai užduodamų klausimų (DUK) skiltis?

2. **Paprastumas**. Ar lengva naudotis paslauga? Kuo sudėtingiau naudoti paslaugą, tuo labiau tikėtina, kad suklysite ir netyčia atskleisite arba prarasite savo informaciją. Rinkitės tokį debesijos paslaugų teikėją, kurio paslaugas lengva suprasti, konfigūruoti ir naudoti.
3. **Saugumas**. Jei renkami kokie nors jūsų duomenys, išsiaiškinkite kokie. Kaip duomenys bus perduodami iš jūsų kompiuterio į debesijos serverį ir kaip jie bus ten laikomi – ar jie bus užšifruoti, o jeigu taip, kas gali juos iššifruoti?
4. **Paslaugų teikimo sąlygos**. Skirkite laiko peržiūrėti paslaugų teikimo sąlygas (dažniausiai jos yra pateikiamos labai paprastai). Peržiūrėkite, kas gali gauti prieigą prie jūsų duomenų ir kokios jūsų juridinės teisės, taip pat, kokius saugumo įsipareigojimus prisiima paslaugų teikėjas, o kokius turėsite prisiimti patys.

Naudodami debesijos paslaugas, prie savo informacijos galite lengviau prisijungti ir tapti produktyvesniais, tačiau būkite atidūs, kokiu būdu prie jos jungiatės ir kaip ja dalijatės.

Kaip apsaugoti savo duomenis?

Pasirinkę debesijos paslaugų teikėją. Tada turėtumėte įsitikinti, kad debesijos paslaugomis naudositės tinkamai. Jūsų pasirinktas prisijungimo prie sistemos ir duomenų dalijimosi būdas gali daryti žymiai didesnį poveikį jūsų failų saugumui, nei visa kita. Todėl pagrindiniai dalykai, į kuriuos vertėtų atsižvelgti, yra šie:

1. **Tapatybės nustatymas**. Norėdami patvirtinti savo debesijos paskyrą, naudokite patikimą ir unikalią slaptafrazę. Jei jūsų debesijos paslaugų teikėjas siūlo naudoti dviejų etapų tapatybės patikrinimą, labai rekomenduojame taip ir daryti. Tai vienas iš svarbiausių veiksmų, kurių galite imtis, siekdami apsaugoti savo paskyrą.
2. **Dalijimasis failais ir aplankais**. Naudojant debesiją, dalytis informacija yra labai paprasta, o kartais net pernelyg paprasta. Blogiausiu atveju, galite manyti, kad savo failais dalijatės tik su konkrečiu asmeniu, tačiau išties netyčia savo dokumentus ar net visus aplankus galite padaryti viešai prieinamus visame internete. Geriausias būdas nuo to apsisaugoti yra nesidalyti savo failais su bet kuo, naudojant numatytus nustatymus. Nustatykite, kad prie konkrečių failų arba aplankų galės prisijungti tik konkretūs žmonės (arba žmonių grupės), kuriems šią informaciją reikia žinoti. Kai niekam nebereiks prisijungti prie šių failų, pašalinkite juos. Jūsų debesijos paslaugų teikėjas turėtų siūlyti paprastą būdą, kuriuo galėtumėte stebėti, kas turi prieigą prie jūsų failų ir aplankų.

Kaip saugiai naudoti debesiją?

3. **Dalijimasis failais ir aplankais per nuorodas**. Vienas iš debesijos paslaugų bendrų bruožų yra galimybė sukurti interneto nuorodą į savo failus arba aplankus. Ši ypatybė leidžia su bet kuo dalytis failais paprasčiausiai nusiunčiant interneto nuorodą. Tačiau šis metodas nėra labai saugus, kadangi prie jūsų asmeninių failų arba aplankų gali prisijungti bet kuris, nuorodą žinantis, asmuo. Jums pasidalijus nuoroda tik su vienu žmogumi, šis asmuo gali ja pasidalyti su kitais arba ją būtų galima rasti naudojant paieškos sistemas. Jei duomenimis dalijatės naudodami nuorodas, įsitikinkite, kad nuorodą išjungsite, kai jos nebereikės, nustatydami jos galiojimo laiką arba, jei tai įmanoma, apsaugodami nuorodą slaptažodžiu.
4. **Nuostatos**. Pasidomėkite, kaip naudoti debesijos paslaugų teikėjo siūlomas saugumo nuostatas. Pavyzdžiui, ar jums su kuo nors pasidalinus aplanku, tie asmenys galės be jūsų žinios jais pakartotinai pasidalyti su dar kuo nors? Taip pat įsitikinkite, ar yra galimybė matyti, kas ir kada peržiūrėjo jūsų pasidalytą turinį. Ar galite apriboti, kad pasidalytą failą kiti galėtų „tik skaityti“, o ne „skaityti ir redaguoti“, jog žmonės negalėtų jų keisti?
5. **Antivirusinė programa**. Įsitikinkite, kad savo ir kituose kompiuteriuose, kuriuos naudodami dalijatės savo duomenimis, esate įdiegę naujausią antivirusinės programos versiją. Užkrėtus failą, kuriuo dalijatės, kiti kompiuteriai, turintys prieigą prie to failo, taip pat gali būti užkrėsti.

SUŽINOKITE DAUGIAU

Prenumeruokite kas mėnesinį OUCH! naujienlaiškį, gaukite prieigą prie archyvų, sužinokite daugiau apie SANS saugumo sprendimus apsilankę securingthehuman.sans.org/ouch/archives.

Šaltiniai

Dviejų etapų tapatybės patikrinimas:	https://securingthehuman.sans.org/ouch/2015#september2015
Slaptafrazės:	https://securingthehuman.sans.org/ouch/2015#april2015
Slaptažodžių tvarkytuvės:	https://securingthehuman.sans.org/ouch/2015#october2015
Kas yra kenkimo programa?:	https://securingthehuman.sans.org/ouch/2016#march2016
SEC524 kursas „Debesijos saugumo pagrindai“:	https://sans.org/sec524

Licencija

Redaktoriai: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Lietuvišką vertimą finansavo „Perlo“ įmonių grupė.