

OUCH!

Backup

Mėnesinis informacinio saugumo naujienlaiškis Tau

Ar pasidarėte atsargines kopijas?

Apžvalga

Jei kompiuterį ar mobilųjį prietaisą naudosite pakankamai ilgai, anksčiau ar vėliau jam kas nors nutiks. Pavyzdžiui, galite netyčia ištrinti reikiamus failus, gali sugesti aparatinė įranga, o gal net pamesite ar kitaip prarasite patį įrenginį. Negana to, jūsų failus gali ištrinti ir (arba) pasisavinti išpirkos reikalaujanti kenkimo programa. Tokiomis akimirkomis atsarginės failų kopijos taps vieninteliu būdu, kuriuo galėsite atkurti savo skaitmeninį gyvenimą.

Kas, kaip ir kur?

Atsarginės kopijos tai bet kur kitur nei kompiuteryje ar mobiliajame prietaise laikomos jūsų informacijos kopijos. Praradus vertingus duomenis, juos galima atkurti iš pasidarytų atsarginių kopijų. Taigi pirmas žingsnis būtų nuspręsti, kokių failų atsargines kopijas norėsite pasidaryti: 1) konkrečių, jums svarbių duomenų ar 2) visų, įskaitant pačią operacinę sistemą. Daugelis atsarginių kopijų darymo sprendimų atsižvelgia į pirmiausiai naudojamus dalykus, taigi bus padarytos dažniausiai naudojamų katalogų atsarginės kopijos. Jei nesate tikri, kokias atsargines kopijas turėtumėte pasidaryti arba norite būti užtikrinti, tuomet darykite visų failų atsargines kopijas.

Toliau turite nuspręsti, kaip dažnai norite daryti atsargines kopijas. Tokios integruotos atsarginių kopijų programos, kaip „Apple Time Machine“ arba „Microsoft Windows Backup and Restore“ leidžia sukurti automatinį „nustatyk ir užmiršk“ principu veikiančią atsarginių kopijų darymo grafiką. Populiariausios parinktys siūlo atsargines kopijas daryti kas valandą, kasdien, kas savaitę ir t.t. Kiti sprendimai siūlo naudotis „pastovia apsauga“, kai yra daromos naujų arba pakeistų failų atsarginės kopijos vos išsaugojus dokumentą. Mes rekomenduojame nustatyti kasdien, automatiškai daryti bent jau svarbiausių failų atsargines kopijas.

Galiausiai, nuspręskite kur laikysite atsargines kopijas. Yra dvi vietos – šalia savęs arba debesijos platformoje. Pirmuoju atveju, atsarginės kopijos būtų laikomos tokiuose jūsų turimuose prietaisuose, kaip išorinė USB laikmena arba per belaidį tinklą pasiekiamas įrenginys. Šio varianto privalumas yra toks, kad tokiu būdu galite greitai daryti didelių duomenų kiekių atsargines kopijas ir taip pat greitai jas atkurti. O trūkumas yra toks, kad jei jūsų įrenginį užkrės išpirkos reikalaujanti kenkimo programa, tuomet tikėtina, jog šis virusas išplis ir į jūsų turimas atsargines kopijas. Be to, atsitikus nelaimei, pavyzdžiui, kilus gaisrui ar įvykus vagystei, galite prarasti ne tik savo kompiuterį, bet ir turėtas atsargines kopijas. Jei atsargines kopijas nusprendėte laikyti išoriniuose įrenginiuose, tuomet juos atitinkamai pažymėkite ir laikykite atokioje bei saugioje vietoje.

Debesijos sprendimai tai internetinės platformos, kuriose bus saugomi jūsų failai. Šiuo atveju, tereikės kompiuteryje įdiegti programą, kuri automatiškai, pagal numatytą grafiką arba vos pakeitus failus, darys atsargines jų kopijas. Debesijos platformų privalumas yra jų naudojimo paprastumas, kadangi failų kopijos dažnai yra daromos automatiškai, o failus galima pasiekti iš bet kurios vietos. Taip pat, kadangi jūsų duomenys bus laikomi debesijoje, padarytų atsarginių kopijų neįtakos tokios namie įvykusios nelaimės kaip gaisras ar vagystė. Galiausiai, laikydami atsargines kopijas debesijos platformoje, galėsite atkurti turėtus failus, jei juos užkoduos išpirkos reikalaujanti kenkimo programa. Šio varianto trūkumas yra tas, kad jūsų galimybės kurti atsargines kopijas ir jas atkurti priklausys nuo duomenų, kuriems buvo sukurtos atsarginės kopijos, kiekio ir tinklo veikimo greičio. Jei nesate tikri, kurį variantą turėtumėte pasirinkti, tuomet, norėdami būti užtikrinti, naudokite abu.

Naudojant mobiliuosius įrenginius, dauguma jūsų duomenų jau yra saugomi debesijos platformose. Tačiau jose gali būti nesaugomi mobiliųjų programų nustatymai, naujausios nuotraukos ir sistemos parinktys. Darant mobiliojo įrenginio duomenų atsargines kopijas, ši informaciją yra ne tik išsaugoma, bet ir lengviau perkeliama, įrenginį keičiant naujesniu.

Esminiai dalykai



- Duomenų atsarginių kopijų darymas yra tik pusė darbo. Dar turite būti tikri, kad galėsite juos atkurti. Periodiškai išbandykite ar veikia jūsų atsarginės kopijos, bandydami failus atkurti ir atidaryti.
- Atkurdami visą sistemą iš atsarginės kopijos, prieš pradėdami ją vėl naudoti, įsitinkite, jog joje įdiegėte naujausias apsaugos pataisas ir atnaujinimus.
- Jei nusprendėte naudoti debesijos sprendimą, pasirinkite tokį, kurį būtų paprasta naudoti ir išnagrinėkite saugumo nustatymus. Pavyzdžiui, ar juose yra dviejų etapų asmens tapatybės patvirtinimas, kuriuo galėtumėte apsaugoti savo internetinę paskyrą.

Atsarginės kopijos tai paprastas ir nebrangus būdas apsaugoti savo skaitmeninį gyvenimą.

Kviestinis redaktorius

Matt Bromiley yra kibernetinės saugos ir reagavimo į incidentus specialistas, dirbantis su įvairių dydžių organizacijomis. Taip pat jis yra SANS instituto dėstytojas, vedantis paskaitas pažengusiems apie reagavimą į serverių ir tinklo incidentus bei organizuojantis kibernetinių grėsmių paieškos pratybas (FOR508 ir FOR572 kursai). Jo veiklą galite stebėti „Twitter“ svetainės paskyroje [@mbromileyDFIR](https://twitter.com/mbromileyDFIR).



Šaltiniai

- Paprastas slaptažodžių kūrimas: <https://www.sans.org/u/TqR>
- Sustabdykime kenkėjiškas programas: <https://www.sans.org/u/TqW>
- Kaip apsaugoti namus nuo kibernetinių pavojų?: <https://www.sans.org/u/Tr1>

OUCH! Yra leidžiamas SANS Security Awareness instituto ir platinamas pagal [Creative Commons BY-NC-ND 4.0 licensiją](https://creativecommons.org/licenses/by-nc-nd/4.0/). Jums leidžiama naudoti ir platinti šį naujienlaiškį su sąlyga, kad niekas nebus keičiama. Norėdami gauti daugiau informacijos susisiekite su mumis www.sans.org/security-awareness/ouch-newsletter. Redaktoriai: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Lietuvišką vertimą finansavo „Perlo“ įmonių grupė.