OUCH! | 2017.gada augusts

Ikmēneša informācijas drošības biļetens ikvienam

OUCH!

ŠAJĀ NUMMURĀ …

Rezerves kopijas un atgūšana

Pārskats

Ja jūs izmantojat datoru vai mobilo ierīci pietiekami ilgi, agrāk vai vēlāk kaut kas sabojājas un tā rezultātā jūsu personiskie faili, dokumenti vai fotoattēli pazūd. Piemēram, jūs varat nejauši izdzēst nepareizos failus, var sabojāties aparatūra, pazust ierīce vai tā tiek inficēta ar ļaunatūru, piemēram, izspiedējvīrusiem. Tādos brīžos rezerves kopijas bieži vien ir vienīgais veids, kā jūs varat atjaunot savu digitālo dzīvi. Šajā izdevumā mēs izskaidrosim, kas ir rezerves kopijas, kā kopēt savus datus un izstrādāt vienkāršu rezerves kopiju veidošanas stratēģiju, kas ir piemērota tieši jums.

Viesredaktors

Keith Palmgren kiberdrošības profesionālis ar vairāk nekā 30 gadu pieredzi informācijas drošības nozarē. Viņš ir SANS institūta vecākais instruktors un SANS SEC301 "Ievadkurss Informācijas drošībā" autors. Keith ir arī sekmīgs drošības konsultants un atrodams arī Twitter **@kpalmgren**.

Rezerves kopijas: kas, kad un kā

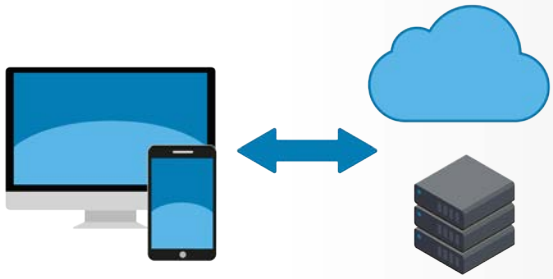
Rezerves kopijas nozīmē, ka jūsu informācija tiek nokopēta un glabājas nevis jūsu datorā vai mobilajā ierīcē, bet kādā citā vietā. Kad jūs zaudējat vērtīgus datus, tos var atgūt no rezerves kopijām. Diemžēl pārāk daudzi neveido rezerves kopijas, pat ja tas ir vienkārši un lēti. Pirmais solis ir izlemt, ko jūs vēlaties saglabāt. Ir divas pieejas: (1) specifiska informācija, kas jums ir svarīga; vai (2) viss, ieskaitot visu jūsu operētājsistēmu. Lielākā daļa risinājumu pēc noklusējuma ir konfigurēti saskaņā ar pirmo pieeju, tie kopē datus no visbiežāk izmantotajām mapēm. Daudzos gadījumos tas ir pilnīgi pietiekami. Tomēr, ja jūs neesat pārliecināts, ko tieši kopēt, vai gribat būt īpaši piesardzīgs, izvēlieties kopēt visu.

Otrkārt, jums jāizvēlas kopēšanas regularitāte. Personīgajiem datoriem iebūvētās rezerves kopēšanas programmas, piemēram, Apple Time Machine vai Microsoft Windows Backup and Restore atļauj jums izveidot automātisku "izveido un aizmirsti" rezerves kopēšanas grafiku. Iespējams izvēlēties kopēt katru stundu, katru dienu, katru nedēļu utml. Citi risinājumi piedāvā "nepārtrauktu aizsardzību", kas nozīmē, ka nekavējoties tiek nokopēti jebkādi izmainītie dati katru reizi, kad jūs saglabājat dokumentu. Mēs iesakam kā minimums automātiskas ikdienas rezerves kopijas.

Visbeidzot ir jāizvēlas, kā jūs veiksiet rezerves kopijas. Ir divi veidi, kā kopēt datus: fizisks datu nesējs vai "mākoņu"

Rezerves kopijas un atgūšana

glabātuve. Katrai pieejai ir savas priekšrocības un trūkumi. Ja nezinat, kādu pieeju izvēlēties, varat lietot abas divas vienlaicīgi. Fiziskie datu nesēji ir iekārtas, ko jūs kontrolējat, piemēram, ārējie USB diski vai tīkla ierīces, kas pieejamas wi-fi tīklā. Jūsu pašu fiziskais datu nesējs ļauj jums kopēt un atjaunot lielus datu apjomus salīdzīnoši ātri. Šādas metodes trūkums ir, ja jūsu datorā ir ļaunatūra, piemēram, izspiedējvīrusi, iespējams, ka tā izplatīsies arī uz rezerves kopijām. Turklāt, ja notiek nelaime, piemēram, ugunsgrēks vai zādzība, jūs varat pazaudēt gan savu datoru, gan rezerves kopijas. Tādēļ, ja jūs izmantojat ārējas iekārtas rezerves kopijām, jums jāplāno glabāt rezerves kopijas citā drošā vietā. Atcerieties arī atbilstoši marķēt rezerves kopiju datu nesējus.



Automātiskas, uzticamas rezerves kopijas bieži ir pēdējā aizsardzības līnija jūsu datiem.

"Mākoņu" glabātuves risinājumi ir tiešsaistes pakalpojumi, kas saglabā jūsu failus Internetā. Parasti jūs instalējat aplikāciju datorā. Aplikācija tad automātiski kopē failus vai nu saskaņā ar grafiku, vai pēc tam, kad jūs veicat izmaiņas. Priekšrocības ir vienkāršība, rezerves kopijas gandrīz vienmēr ir automātiskas un jūs varat piekļūt tām no jebkuras vietas. Turklāt jūsu dati glabājas mākonī, tādēļ ugunsgrēks vai zādzība mājās neietekmēs jūsu rezerves kopijas. Trūkumi ir tas, ka kopiju veidošana un arī atgūšana var prasīt ilgāku laiku, īpaši ja datu apjoms ir liels. Svarīgi arī ir privātuma un drošības apsvērumi. Vai rezerves kopiju pakalpojuma sniedzējs nodrošina drošības kontroles, piemēram, datu šifrēšanu un drošu autentifikāciju?

Neaizmirstiet arī par mobilajām ierīcēm. Mobilajās ierīcēs vairums jūsu datu – e-pasts, kalendārs, kontakti jau tiek glabāti mākonī. Tomēr jūsu aplikāciju iestatījumi, nesenie foto un sistēmas iestatījumi ne vienmēr tiek saglabāti. Veidojot rezerves kopijas mobilai ierīcei, jūs ne tikai saglabājat informāciju, bet arī atvieglojat pāreju uz jaunu ierīci. iPhone/iPad var automātiski veidot rezerves kopijas Apple iCloud. Android un citas ierīces iestatījumi ir dažādi atšķirīgiem ražotājiem. Dažos gadījumos Jūs varat iegādāties aplikācijas, kas tieši domātas rezerves kopiju veidošanai.

Atgūšana

Rezerves kopiju veidošana ir tikai daļa no cīņas, jums nepieciešams arī atgūt datus. Periodiski pārbaudiet, vai jūsu rezerves kopijas strādā, atgūstiet kādu failu un pārbaudiet informāciju. Noteikti izveidojiet pilnu sistēmas rezerves kopiju pirms lielām

Rezerves kopijas un atgūšana

izmaiņām (piemēram, pārejot uz jaunu datoru vai mobilo iekārtu) vai remontdarbiem (piemēram, aizstājot cieto disku) un pārbaudiet vai sistēma ir atjaunojama.

Pamata lietas

- Lai kādu risinājumu izmantojat, veidojiet rezerves kopijas automātiski un regulāri pārbaudiet tās.
- Atjaunojot sistēmu no rezerves kopijām, atkārtoti uzstādiet jaunākos drošības ielāpus un atjauninājumus pirms sistēmas izmantošanas.
- Vecas rezerves kopijas, kas nav vairāk nepieciešamas, ieteicams iznīcināt, lai tām nepiekļūtu neautorizētas personas.
- Ja jūs izmantojat "mākoņa" risinājumu, izpētiet pakalpojuma sniedzēja nosacījumus un reputāciju un izvērtējiet, vai tas atbilst jūsu prasībām. Piemēram, vai dati tiek šifrēti? Kurš var piekļūt jūsu kopijām? Vai pakalpojumu sniedzējs nodrošina drošu autentifikāciju, piemēram, divu faktoru verifikāciju?

UZZINIET VAIRĀK

Parakstieties uz OUCH! - ikmēneša biļetenu par informācijas tehnoloģiju drošību datoru lietotājiem, apmeklējiet OUCH! arhīvu, uzziniet vairāk par SANS informācijas tehnoloģiju drošības risinājumiem, apmeklējot tīmekļa vietni securingthehuman.sans.org/ouch/archives.

CERT.LV ir Latvijas Republikas Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. CERT.LV misija ir veicināt informācijas tehnoloģiju drošību Latvijā. Uzziniet vairāk https://www.cert.lv vai sekojiet mums Twiterī @certlv.

Resursi

Paroļu frāzes:	https://securingthehuman.sans.org/ouch/2017#april2017
Divu faktoru verifikācija:	https://securingthehuman.sans.org/ouch/2015#september2015
Mākoņa drošība:	https://securingthehuman.sans.org/ouch/2016#november2016
Šifrēšana:	https://securingthehuman.sans.org/ouch/2016#june2016
Izspiedējvīrusi:	https://securingthehuman.sans.org/ouch/2016#august2016

License

Redakcija: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Tulkojums: Edgars Tauriņš