OUCH! 2022 - 09


# Rezerves kopijas gatavas?

## Pārskats

Ilgstošu laiku lietojot datoru vai mobilo ierīci, agri vai vēlu kaut kas noies greizi. Var gadīties nejauši izdzēst vajadzīgās datnes, var rasties aparatūras kļūme vai arī ierīce var tikt nozaudēta. Vai pat vēl sliktāk – datnes var inficēt un dzēst vai šifrēt ļaunprogrammatūra. Šādos brīžos rezerves kopijas bieži vien ir vienīgais veids, kā atjaunot savu digitālo dzīvi.

Rezerves kopijas ir informācijas kopijas, kas glabājas kādā citā vietā, nevis datorā vai mobilajā ierīcē. Kad gadās pazaudēt vērtīgus datus savā ierīcē vai tiem vairs nav iespējams piekļūt, datus var atgūt no rezerves kopijām. Daudzas no šodien izveidojamām datnēm jau tiek automātiski saglabātas un tām tiek veidotas rezerves kopija mākonī, piemēram, Microsoft Word dokumenti var tikt saglabāti Microsoft OneDrive, Dropbox vai Google Drive, personīgie fotoattēli – Apple iCloud. Taču var būt arī tādas datnes, kas netiek automātiski saglabātas mākonī; vai arī ir nepieciešamas papildu rezerves kopijas personīgai lietošanai.

## Ko, kad un kā

Pirmais solis ir izlemt, kas ir iekļaujams rezerves kopijā: (1) konkrēti svarīgi dati; vai arī (2) viss – iespējams, ieskaitot arī visu operētājsistēmu. Daudzi rezerves kopiju veidošanas risinājumi pēc noklusējuma ir konfigurēti pirmajam variantam un rezerves kopijas veido tikai visbiežāk izmantotām mapēm. Ja nav pilnīgas pārliecības par to, kam ir nepieciešama rezerves kopija, vai arī ja ir nepieciešama īpaša uzmanība, ir vērts apsvērt iespēju veidot rezerves kopiju visam.

Pēc tam ir jāizlemj, cik bieži dublēt datus. Iebūvētās rezerves kopēšanas programmas, piemēram, Apple Time Machine vai Windows Backup and Restore, ļauj izveidot automātisku “iestatīt un aizmirst” grafiku. Bieži izmantojamie varianti ir saglabāšana reizi stundā, dienā vai nedēļā. Citi risinājumi var piedāvāt "nepārtrauktu aizsardzību" - šajā gadījumā datnes tiek nekavējoties dublētas, tiklīdz tās ir rediģētas vai saglabātas. Ieteikums būtu veikt automātisku kritiski svarīgo datņu rezerves kopēšanu vismaz reizi dienā.
Un visbeidzot, ir jāizlemj, kā veikt rezerves kopēšanu. Pastāv divi veidi: vietējās vai mākonī saglabātās rezerves kopijas. Vietējās rezerves kopijas ir atkarīgas no fiziski kontrolējamām ierīcēm, piemēram, ārējām USB zibatmiņām vai tīklā pieejamām ierīcēm. Vietējo rezerves kopiju priekšrocība ir tā, ka tās ļauj ātri dublēt un atgūt lielu datu apjomu. Trūkums ir tāds, ka, inficēšanās gadījumā ar ļaunprogrammatūru, infekcija var izplatīties arī rezerves kopijās. Un nelaimes gadījumā, piemēram, ja notiek ugunsgrēks vai zādzība, var zaudēt gan datoru, gan rezerves kopijas.
Izmantojot rezerves kopēšanai ārējās ierīces, ir vērts glabāt rezerves kopijas citā drošā vietā un skaidri tās apzīmēt. Papildu drošībai var apsvērt iespēju šifrēt rezerves kopijas.

Mākoņa risinājumi ir tiešsaistes pakalpojumi, kas dublē un saglabā datnes internetā. Parasti datorā tiek instalēta lietojumprogrammatūra. Pēc tam tā automātiski veido datņu rezerves kopijas vai nu pēc noteikta grafika, vai arī modificējot vai saglabājot šīs datnes. Dažas mākoņa risinājumu priekšrocības ir to vienkāršība, rezerves kopēšanas automatizācija un piekļuve datnēm gandrīz no jebkuras vietas. Turklāt, tā kā dati atrodas mākonī, mājas katastrofas, piemēram, ugunsgrēks vai zādzība, neietekmēs rezerves kopijas. Galvenais šī risinājuma trūkums ir patērētais joslas platums. Iespēja veikt rezerves kopēšanu un atjaunot datus ir atkarīga no dublējamā datu daudzuma un tīkla ātruma. Nav pārliecības par to, vai izmantot vietējo rezerves kopēšanu vai darīt to mākonī? Izvēlieties īpaši drošu pieeju – izmantojiet gan vienu, gan otru.

Izmantojot mobilās ierīces, lielākā daļa datu, piemēram, e-pasta ziņojumi, īsziņas vai uzņemtie fotoattēli, tiek automātiski saglabāti mākonī. Taču mobilo lietotņu konfigurācijas, sistēmas iestatījumi un citas datnes var netikt saglabātas mākonī. Veicot mobilās ierīces automātisko rezerves kopēšanu, tiek ne vien saglabāta informācija, bet arī pārejot uz jaunas ierīces lietošanu, ir vieglāk tajā pārsūtīt saglabātos datus.

## Svarīgas piezīmes

- Rezerves kopiju darbspēja ir regulāri jāpārbauda, izgūstot un atverot datni.
- Atjaunojot sistēmu no rezerves kopijas, tostarp operētājsistēmu, pirms tās izmantošanas ir noteikti atkārtoti jāpielieto jaunākie drošības ielāpi un atjauninājumi.
- Izmantojot mākoņa risinājumu, ir vērts izvēlēties tādu, kas ir ērti lietojams, un izpētīt piedāvātās drošības iespējas. Piemēram, vai mākoņa rezerves kopēšanas piegādātājs atbalsta divpakāpju verifikāciju lietotāja tiešsaistes konta aizsardzībai?

Rezerves kopijas ir vienkāršs un lēts veids savas digitālās dzīves aizsardzībai.

## Viesredaktors

Gregs Šaidels (Greg Scheidel) ir Iron Vine Security galvenais informācijas drošības speciālists ar vairāk nekā 30 gadu pieredzi IT un IT drošības jomā. Viņš ir arī SANS instruktors un pasniedz drošības arhitektūru, inženieriju un nulles uzticēšanos SEC530. Ar viņu var sazināties Twitter @greg_scheidel.

## Resursi

**Divu faktoru autentifikācija:** https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/
**Droša mākoņa lietošana:** https://www.sans.org/newsletters/ouch/securely-using-mobile-apps/
**Paroļu pārvaldītāji:** https://www.sans.org/newsletters/ouch/password-managers/
**Digitālais mantojums:** https://www.sans.org/newsletters/ouch/digital-inheritance/

**Tulkojums: CERT.LV**