Ikmēneša Informācijas drošības izdevums Tev

Vai tev ir rezerves kopijas?

Pārskats

Ja jūs izmantosiet datoru vai mobilo iekārtu pietiekami ilgi, agrāk vai vēlāk notiks kaut kas slikts. Jūs varat netīšām izdzēst nepareizos failus, var notikt tehniska kļūme, vai var gadīties, ka pazaudējat iekārtu. Vai pat ļaunāk, ļaunatūra, tāda kā izspiedējvīruss, var izdzēst jūsu failus un/vai pārņemt pār tiem kontroli. Šādos brīžos rezerves kopijas bieži vien ir vienīgais veids kā atjaunot savu digitālo dzīvi.

Kas, kad, kā?

Rezerves kopijas (backups) ir jūsu informācijas kopijas, kas tiek glabātas kaut kur citus, nevis jūsu datorā vai mobilajā iekārtā. Ja jūs pazaudējat vērtīgu informāciju, jūs varat to atjaunot no rezerves kopijām. Pirmais solis ir saprast, ko jūs vēlaties saglabāt/ kopēt, (1) specifiskus datus, kas jums ir svarīgi; vai (2) pilnīgi visu, ieskaitot jūsu iekārtas operētājsistēmu. Daudzi rezerves kopiju sagatavošanas risinājumi pēc noklusējuma ir nokonfigurēti atbilstoši pirmajai pieejai, tie kopē visbiežāk izmantotās mapes (folders). Ja neesat droši, kam vēlaties veidot rezerves kopijas, vai vēlaties ievērot īpašu piesardzību, veidojiet rezerves kopijas visam.

Otrais, izvēlieties, cik bieži veidot rezerves kopijas. Iebūvētie rezerves kopiju veidošanas risinājumi, tādi kā Apple Time Machine vai Windows Backup and Restore ļauj jums uzstādīt automātisko grafiku. Visbiežākie varianti iekļauj ik stundas, ik dienas, ik nedēļas u.c. kopēšanu. Citi risinājumi piedāvā “nepārtrauktu aizsardzību”, kurā jauni vai modificēti faili tiek tūlītēji kopēti katru reizi, kad veicat dokumenta saglabāšanu. Kā minimums, mēs iesakām automātiski kopēt visus svarīgos failus reizi dienā.

Visbeidzot, izvēlieties, kā jūs glabāsiet rezerves kopijas. Ir divas iespējas: glabāt lokāli vai mākonī. Lokālajām rezerves kopijām tiek izmantotas iekārtas, kuras jūs kontrolējat, tādas kā ārējais cietais disks vai tīkla disks. Lokālā varianta priekšrocība ir iespēja gan ātri nokopēt, gan atjaunot lielu datu apjomu. Trūkums ir, ja jūs tiekat inficēts ar šifrējošo izspiedējvīrusu (ransomware), iespējams, ka infekcija piekļūs arī jūsu rezerves kopijām. Arī gadījumos, kad jūs piemeklē kāda nelaime, piemēram, zādzība vai ugunsgrēks, jūs varat zaudēt gan jūsu datoru, gan rezerves kopijas. Ja rezerves kopijām izmantojat ārējas iekārtas, glabājiet kopiju kādā fiziski atšķirīgā, drošā vietā, un pārliecinieties, ka jūsu rezerves kopijas tiek kārtīgi marķētas.

Mākoņrisinājumi ir tiešsaistes servisi, kas glabā jūsu failus internetā. Parasti jūs savā datorā lejupielādējat un instalējat lietotni, kas veido rezerves kopijas vai nu automātiski, atbilstoši uzstādītajam grafikam, vai tad, kad veicat izmaiņas failos. Mākoņrisinājumu

priekšrocība ir to vienkāršība, rezerves kopēšana bieži vien ir automātiska un jūs varat piekļūt saviem datiem no jebkurienes. Un, tā kā jūsu dati dzīvo mākonī, nekādas mājas nelaimes, tādas kā ugunsgrēks vai zagļi tos neapdraud. Visbeidzot, mākonī glabātas rezerves kopijas palīdzēs jums atgūties no ļaunatūras uzbrukuma, piemēram, šifrējošā izspiedējvīrusa infekcijas. Trūkums ir tāds, ka jūsu iespējas veidot rezerves kopijas un attiecīgi atjaunot datus var būt ierobežotas datu apjomā, un ir atkarīgas no jūsu tīkla pārraides ātruma. Neesat droši, vai vēlaties izmantot rezerves kopijām lokālo vai mākoņrisinājumu? Esiet īpaši droši un izmantojiet abus!

Izmantojot mobilo iekārtu, lielākā daļa jūsu datu jau tiek glabāta mākonī. Taču jūsu mobilo lietotņu iestatījumi, nesenas fotogrāfijas un sistēmiestatījumi var nebūt. Izveidojot savas mobilās iekārtas rezerves kopiju, jūs ne tikai saglabāsiet šo informāciju, bet būs vienkāršāk nomigrēt datus uz jaunu iekārtu, ja tas būs nepieciešams.

Galvenās atziņas

- **Rezerves kopijas izveidošana ir tikai pusceļš; jums ir jāpārliecinās, ka tā ir izmantojama. Regulāri pārbaudiet, ka jūsu rezerves kopijas ir izmantojamas, sameklējot un atverot failu.**
- **Ja atjaunojat sistēmu no rezerves kopijas, pārliecinieties, ka uzstādiet jaunākos drošības ielāpus un atjauninājumus pirms uzsāciet to lietot.**
- **Ja izmantojiet mākoņrisinājumu, izvēlieties vienu, kuru jums ir ērti lietot, un izpētiet drošības iespējas. Piemēram, vai viņi piedāvā divu faktoru verifikāciju jūsu konta drošībai?**

Rezerves kopijas ir vienkāršs un lēts risinājums jūsu digitālās dzīves aizsardzībai.

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.

Viesredaktors

Matt Bromiley *ir kiberdrošības profesionālis un incidentu risinātājs, kas ir strādājis ar dažāda lieluma organizācijām. Viņš ir arī SANS instruktors, kas pasniedz padziļinātu resursdatoru (host) un tīklu incidentu risināšanu un apdraudējum novēršanu FOR508 un FOR572. Jūs varat viņu sastapt Twitter* @mbromileyDFIR.

Resursi

Kā padarīt paroles vieglāk iegaumējamas:	https://www.sans.org/u/TqR
Stāties pretī ļaunatūrai:	https://www.sans.org/u/TqW
Mājas kiberdrošība:	https://www.sans.org/u/Tr1

Redakcija: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Tulkojums: CERT.LV