Publicația dumneavoastră lunară de sensibilizare asupra securității informatice

Aveți backup?

Prezentare generală

Dacă utilizați un computer sau un dispozitiv mobil timp îndelungat, mai devreme sau mai târziu ceva va merge prost. Ori ștergeți anumite fișiere din greșeală, ori vi se strică hardware-ul sau poate chiar pierdeți dispozitivul. Și mai rău, programele malware, cum ar fi ransomware, vă pot șterge fișierele și / sau vă pot bloca accesul la ele. În astfel de momente, backup-urile sunt adesea singura modalitate prin care vă puteți reconstrui viața digitală.

Ce, când și cum

Backup-urile sunt copii ale informațiilor stocate undeva, în altă parte decât pe computerul dvs. sau pe dispozitivul mobil. Când pierdeți informații importante, le puteți recupera din aceste copii de rezervă. Primul pas este să decideți la ce doriți să faceți backup, (1) anumite informații și fișiere care sunt importante pentru dvs.; sau (2) totul, inclusiv întregul sistem de operare. Multe soluții de backup sunt configurate în mod implicit pentru a utiliza prima abordare, făcând backup la cele mai frecvent utilizate fișiere. Dacă nu sunteți sigur(ă) la ce să faceți backup sau doriți să fiți foarte precaut(ă), faceți backup la tot.

Următorul pas este să decideți cât de frecvent veți face copiile de rezervă. Programele de backup încorporate, cum ar fi Time Machine de la Apple sau Windows Backup and Restore vă permit să activați programul automat “setați-l și uitați-l”. Opțiunile comune sunt din oră în oră, zilnic, săptămânal, etc. Alte soluții oferă o “protecție continuă” în care se face backup automat de fiecare dată când salvați un document. Vă recomandăm cel puțin un backup automat zilnic al fișierelor critice.

În cele din urmă, decideți cum veți face backup-ul. Există două metode: stocare într-un spațiu local sau în cloud. Backup-urile locale se bazează pe dispozitive pe care le controlați, cum ar fi USB-uri sau dispozitive accesibile prin wifi. Avantajul este că vă permit să copiați și să recuperați rapid cantități mari de date. Dezavantajul este că dacă veți fi infectat cu programe malware, cum ar fi ransomware-ul, este posibil ca infecția să se răspândească și la copiile de rezervă. De asemenea, un dezastru cum ar fi incendiu sau furt, poate duce la pierderea nu numai a computerului, ci și a copiilor de rezervă. Dacă utilizați dispozitive externe pentru copii de rezervă, stocați o copie într-o altă locație sigură și asigurați-vă că copiile de rezervă sunt etichetate corespunzător.

Soluțiile bazate pe cloud sunt servicii online care vă stochează fișierele pe internet. În mod normal, instalați o aplicație pe computerul dvs., aplicația apoi vă salvează automat fișierele, fie conform unui orar prestabilit fie pe măsură ce le modificați.

Un avantaj al soluțiilor cloud este simplitatea lor, backup-urile sunt adesea automate și de obicei vă puteți accesa fișierele de oriunde. De asemenea, deoarece datele dvs. se află în cloud, dezastre cum ar fi un incendiu sau un furt, nu vă vor afecta backup-ul. În cele din urmă, backup-urile cloud vă pot ajuta să vă recuperați în urma unor infecții malware, cum ar fi ransomware-ul. Dezavantajele ar fi abilitatea dvs. de a face backup-ul, iar restaurarea fișierelor depinde de mărimea datelor copiate și de viteza rețelei. Nu sunteți sigur(ă) care dintre soluții să folosiți, local sau cloud? Fiți extra precaut(ă) și utilizați ambele.

În cazul dispozitivelor mobile, majoritatea datelor dvs. sunt deja stocate în cloud. Cu toate acestea, configurațiile aplicațiilor dvs., fotografiile recente sau preferințele din setări ar putea să nu fie. Dacă efectuați un backup al dispozitivului mobil, nu numai că păstrați aceste informații, dar va fi mult mai ușor să transferați datele când vă schimbați dispozitivul.

Puncte cheie

- **Efectuarea backup-ului este doar jumătate din drum; trebuie să fii sigur și că puteți recupera datele. Testați periodic backup-urile, încercând să recuperați și deschideți un fișier la întâmplare.**
- **Dacă reconstruiți un sistem din copia de siguranță, aplicați ultimele patch-uri și actualizări de securitate înainte de a-l utiliza.**
- **Dacă utilizați o soluție de tip cloud, selectați una ușor de utilizat și studiați-i opțiunile de securitate înainte. De exemplu, vedeți dacă folosește verificarea în doi pași pentru asigurarea contului online.**

Backup-urile sunt o modalitate simplă și ieftină de a vă proteja viața digitală.

Versiunea în limba română

Ubisoft este o companie de jocuri. Un creator de lumi, dedicat îmbogățirii vieților jucătorilor cu experiențe de joc originale și memorabile. Alflați mai multe la: https://www.ubisoft.com/en-us/.

Editor invitat

Matt Bromiley *este un profesionist în domeniul securității și incidentelor informatice care a lucrat cu organizații de toate mărimile. Este, de asemenea, profesor la Institutul SANS, unde predă cursurile avansate FOR508 și FOR572 despre găzduire web (hosting), răspuns la incidente de rețelistică si urmărirea de amenințări cibernetice. Îl puteți găsi si pe Twitter @mbromileyDFIR.*

Resurse

Simplificarea parolelor:	https://www.sans.org/u/Sd8
Securizarea dispozitivului mobil personal:	https://www.sans.org/u/Sdd
Opriți programele Malware:	https://www.sans.org/u/Sdi