OUCH! 2022. szeptember

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Rendelkezünk biztonsági mentésekkel?

Áttekintés

Ha elég hosszú ideig használunk egy számítógépet vagy mobiltelefont, biztosak lehetünk benne, hogy előbb vagy utóbb valami baj fog történni az eszközzel. Például véletlenül rossz fájlt törlünk ki, valamilyen hardverhiba lép fel vagy egyszerűen elveszítjük a készüléket. Az is előfordulhat, hogy káros szoftverek fertőzik meg az eszközünket, amelyek törlik vagy titkosítják a fájljainkat. Ilyen esetekben a biztonsági mentés az egyetlen módja digitális életünk újjáépítésének.

A biztonsági mentések (backupok) adataink olyan másolatai, amelyeket nem a számítógépünkön vagy telefonunkon tárolunk. Így ha a számunka értékes adatainkat elveszítjük, vagy nem férünk hozzájuk az eszközünkön, akkor helyreállíthatjuk azokat a biztonsági mentésekből. Az általunk létrehozott fájlok nagy része ma már automatikusan mentésre kerül a felhőben, mint például azok a Microsoft Word dokumentumaink, amelyeket a OneDrive-ban, a Dropbox-on vagy Google Drive-on tárolunk, vagy például az Apple felhőjében, az iCloud-on őrzött képeink. Előfordulhat azonban, hogy a felhőszolgáltató bizonyos fájlokat nem tárol el automatikusan, vagy esetleg további személyes használatú mentéseket szeretnénk létrehozni.

Mit, mikor és hogyan?

Legelső lépésként döntsük el, hogy miről szeretnénk biztonsági mentést készíteni: (1) kizárólag bizonyos adatokról, amelyek igazán fontosak a számunkra; vagy (2) minden adatról, és akár az egész operációs rendszerről. Számos backup megoldás alapértelmezett beállítás szerint az első megközelítést alkalmazza, és csak a leggyakrabban használt mappákról készít biztonsági másolatot. Ha nem vagyunk biztosak abban, hogy mely adatokat szeretnénk lementeni, vagy csak szeretnénk extra elővigyázatosak lenni, megfontolandó, hogy mindenről készítsünk egy biztonsági mentést.

A következő lépésben döntsük el, hogy milyen gyakorisággal készüljön biztonsági mentés. Léteznek úgynevezett beépített biztonsági mentési programok, például az Apple Time Machine vagy a Windows Backup and Restore funkciója, amelyekkel automatikus ütemezést hozhatunk létre. Gyakori időzítési lehetőségek közé tartozik az óránkénti, napi és heti ütemezés. Léteznek olyan megoldások, amelyek „folyamatos védelmet” kínálnak, ilyenkor a fájlok szerkesztése vagy mentése után azonnal készül egy biztonsági másolat. A kritikus fájlok esetében legalább a napi automatikus mentés beállítása javasolt.
Végezetül döntsük el, hogy hogyan szeretnénk biztonsági másolatot készíteni, ez lehet helyi vagy felhőalapú! A helyi biztonsági mentések olyan eszközökre támaszkodnak, amelyek fizikailag is az irányításunk alatt állnak, ilyenek például a külső USB-meghajtók vagy a hálózaton elérhető eszközök. Ezek előnye, hogy lehetővé teszik nagy mennyiségű adat gyors mentését és helyreállítását. Hátrányuk azonban, hogy ha eszközünk káros programokkal fertőződik meg, előfordulhat, hogy a vírus átterjedhet a biztonsági másolatokra. Továbbá, az olyan szerencsétlen esetekre is gondolnunk kell, mint például ha tűz üt ki otthon vagy betörnek hozzánk, amelyek során elveszíthetjük a számítógépünket és a biztonsági másolatainkat.

Ha egy külső eszközt használunk az adatmentéshez, javasolt erről egy másolatot készíteni, és azt egy biztonságos helyen tartani. Egy jó tanács: ne feledjük el felcímkézni a másolatot! A további biztonság érdekében fontoljuk meg a biztonsági másolatok titkosítását!

A felhőalapú megoldások olyan online szolgáltatások, amelyek az Interneten tárolják a lementett fájlokat. Ezeknél jellemzően egy applikációt kell telepítenünk a számítógépünkre. Az alkalmazás ezután automatikusan biztonsági mentést készít a fájlokról, akár egy előre meghatározott ütemterv szerint, vagy amikor módosítjuk és mentjük őket. A felhőalapú megoldások előnye leginkább az egyszerűségben és az automatizált adatmentésekben rejlik, illetve további pozitívum, hogy az adatainkhoz szinte bárhonnan hozzáférhetünk. Mivel minden adatunk a felhőben kerül tárolásra, így az otthoni katasztrófák, például egy váratlan tűz vagy lopás nem veszélyeztetik a biztonsági mentésünket. Fő hátrányuk az általuk igénybevett hálózati sávszélesség. A mentett adatmennyiség mérete és a hálózatunk sebessége is befolyásolja a biztonsági mentések elkészítését, valamint az adatok visszaállítását is. Nem tudunk választani a helyi és a felhőalapú mentések közül? Legyünk extra biztonságosak és használjuk mindkettőt!

Mobilkészülék esetén a legtöbb adatunk, mint például az e-mailek, SMS-ek, vagy a fényképeink automatikusan mentésre kerülnek a felhőbe. Előfordulhat azonban, hogy a mobilapplikáció konfigurációk, rendszerbeállítások vagy egyéb fájlok nem tárolódnak el a felhőben. A mobilkészülékről készített automatikus biztonsági mentésekkel nem csupán megőrizhetjük ezeket az információkat, de új készülék esetén is sokkal könnyebb lesz az adatátvitel.

További kulcsfontosságú lépések

- Rendszeresen ellenőrizzük, hogy biztonsági mentéseink működnek-e, amit legegyszerűbben egy fájl visszakeresésével és megnyitásával tehetünk meg!
- Ha egy biztonsági mentésből az operációs rendszert is visszaállítjuk, arra is fordítsunk figyelmet, hogy a legújabb biztonsági javításokat és frissítéseket is telepítsük!
- Felhőalapú megoldás esetén válasszunk olyat, ami számunkra könnyen használható, illetve nézzünk utána annak, hogy ez a megoldás milyen kiegészítő biztonsági lehetőségeket kínál! Például a szolgáltató támogatja a kétlépcsős azonosítást online fiókunk biztonsága érdekében?

A biztonsági mentések egyszerű és költséghatékony megoldást nyújtanak digitális életünk védelméhez.

A szerzőről

Greg Scheidel az Iron Vine Security kiberbiztonsági igazgatója, aki több mint 30 éves informatikai és IT-biztonsági tapasztalattal rendelkezik. Emellett a SANS oktatója is, a SEC530 kurzus keretében biztonsági architektúráról és tervezésről, valamint a Zero Trust biztonsági modellről tart előadásokat. Twitteren a @greg_scheidel fiók alatt érhető el.

Források

Többfaktoros autentikáció: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/
A „felhő" biztonságos használata: https://www.sans.org/newsletters/ouch/securely-using-the-cloud/
Jelszókezelők: https://www.sans.org/newsletters/ouch/password-managers/
Digitális öröklés: https://www.sans.org/security-awareness-training/resources/digital-inheritance

A fordítást készítette: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)