Az Ön havi biztonságtudatossági hírlevele

Rendelkezik biztonsági mentéssel?

Áttekintés

Ha elég régóta használ egy számítógépet vagy mobil eszközt, előbb vagy utóbb valami el fog romlani, például véletlenül törölhet egy fájlt, meghibásodhat a hardver, esetleg elveszítheti az eszközét. Még rosszabb, hogy egy rosszindulatú szoftver, mint például egy zsarolóvírus törölheti a fájljait és / vagy titkosíthatja azokat. Az ilyen esetekben gyakran a biztonsági mentés az egyetlen lehetőség digitális életének újjáépítésére.

Mit, Mikor és Hogyan

A biztonsági mentések az Ön adatainak olyan másolatai, amelyek nem a számítógépén, illetve mobileszközén kerülnek tárolásra. Amikor értékes adatai elvesznek, a biztonsági mentésből helyreállíthatja azokat. Az első lépés annak eldöntése, hogy mit szeretne menteni: (1) különleges adatokat, amelyek fontosak Önnek, vagy (2) mindent, beleértve az operációs rendszert is. Számos mentési megoldás úgy van beállítva, hogy alapértelmezettként az első megközelítést alkalmazza és a leggyakrabban használt mappákról készít biztonsági mentést. Amennyiben nem biztos benne, hogy miről kellene biztonsági mentést készítenie, vagy igazán elővigyázatos szeretne lenni, mentsen el mindent.

Második lépésként határozza meg a biztonsági mentés gyakoriságát. Az olyan beépített adatmentő programok, mint például az Apple-féle Time Machine, vagy a Windows Biztonsági mentés és visszaállítás funkciója lehetővé teszik az automatikus „állítsa be és felejtse el” ütemezés használatát. Gyakori lehetőségek az óránkénti, napi, heti, stb. mentések. Más megoldások „folyamatos védelmet” ajánlanak, amelyek esetén az új, vagy a módosított fájlokról minden alkalommal, azonnal biztonsági mentés készül, amikor Ön elment egy dokumentumot. Azt javasoljuk, hogy legalább a kritikus fájlokról készítsen automatikus, napi biztonsági mentést.

Végül, döntse el, hogy hol tárolja biztonsági mentését. Két lehetőség létezik: a helyi vagy a felhő alapú tárolás. A helyi biztonsági mentések az Ön felügyelete alatt álló külső USB meghajtókra vagy Wi-Fi-s hálózati eszközökre támaszkodnak. A helyi tárolás előnye, hogy lehetővé teszi nagy mennyiségű adatok gyors biztonsági mentését és visszaállítását. Hátránya, hogy ha rendszere rosszindulatú szoftverrel, mint például egy zsarolóvírussal fertőződik meg, a fertőzés átterjedhet a biztonsági mentéseire is. Ha netán katasztrófa éri Önt, mint például tűzkár vagy lopás, a számítógépével együtt a biztonsági mentései is elveszhetnek. Ha külső adattárolót használ, egy másolatot tartson belőle egy távoli, biztonságos helyen és győződjön meg arról, hogy a biztonsági másolatok megfelelően vannak felcímkézve.

A felhő alapú megoldások olyan online szolgáltatások, amelyek az Ön fájljait az Interneten tárolják. Általában ez úgy működik, hogy feltelepít egy alkalmazást a számítógépére, és ez az alkalmazás automatikusan biztonsági mentést készít a fájljairól egy meghatározott ütemterv szerint, vagy akkor, amikor módosítja azokat. A felhő alapú tárolás előnye az

egyszerűség: a biztonsági mentés gyakran automatikus, és a fájljait általában bárhonnan el tudja érni. Mivel adatai a felhőben tárolódnak, az otthoni katasztrófák, mint például tűzkár vagy lopás nincsenek hatással a biztonsági mentésére. Végezetül, a felhő alapú biztonsági mentések segíthetnek Önnek egy rosszindulatú szoftver, mint például zsarolóvírus fertőzés után visszaállítani az adatokat. A megoldás hátránya, hogy a biztonsági mentés és visszaállítás lehetősége nagyban függ az adatok mennyiségétől és az Ön hálózatának sebességétől. Nem biztos benne, hogy a helyi és a felhő alapú biztonsági mentés közül melyiket válassza? Törekedjen az extra biztonságra, használja mindkettőt.

Mobil eszközök esetében adatainak nagy része már felhőben tárolódik. Azonban előfordulhat, hogy az alkalmazások beállításai, az új fényképek és rendszer beállítások már nem. A mobilkészülék biztonsági mentésével nemcsak megőrzi ezeket az adatokat, hanem könnyebbé teszi adatainak átvitelét, amikor egy újabb eszközre vált.

Főbb pontok

- **Adatainak biztonsági mentése csak fél siker: rendszeresen bizonyosodjon meg róla, hogy vissza is tudja állítani azokat. Időnként a fájlok visszakeresésével és megnyitásával próbálja ki, hogy biztonsági mentése valóban működik.**
- **Amennyiben biztonsági mentésből állítja vissza rendszerét, annak ismételt használata előtt győződjön meg a legfrissebb hibajavító csomagok és frissítések meglétéről.**
- **Ha felhő alapú megoldást használ, olyat válasszon, amit könnyen tud használni, és ismerje meg a biztonsági beállításait is. Például, hogy támogatják-e a kétfaktoros azonosítást, online fiókjának védelme érdekében.**

A biztonsági mentés egyszerű és költséghatékony módja annak, hogy megvédje digitális életét.

Magyar Kiadás

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) látja el Magyarországon az állami és önkormányzati szervek vonatkozásában az elektronikus információbiztonsági hatósági, eseménykezelési, valamint a sérülékenység-vizsgálati feladatokat. Az NKI rendeltetése, hogy előmozdítsa a kormányzati szektor elektronikus informatikai rendszerei biztonsági szintjének emelését, valamint, hogy fejlessze a közigazgatásban dolgozó felhasználók biztonságtudatos viselkedését a kibertérben. A nemzetközi és hazai partnerkapcsolatai révén az NKI hozzájárul a magyar kibertér biztonságának erősítéséhez. További információ az Intézetről a https://nki.gov.hu oldalon olvasható.

A szerzőről

Matt Bromiley *kiberbiztonsági szakértő és incidenskezelő, munkája során különböző méretű szervezetekkel dolgozott már együtt. SANS oktató, aki a FOR508 és a FOR572 haladó szintű hoszt és hálózati incidenskezelés, fenyegetésvadászat tanfolyamokon oktat. Elérhető Twitteren a @mbromileyDFIR felhasználói néven.*

Források

Egyszerű jelszókezelés:	https://www.sans.org/u/TqR
Káros kódok megállítása:	https://www.sans.org/u/TqW
Kiberbiztonságos otthon létrehozása:	https://www.sans.org/u/Tr1