Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadásban...

- **Mikor és miről készítsünk biztonsági mentést?**
- **Hogyan készítsük el?**
- **Helyreállítás**
- **Fontos lépések**

Biztonsági mentés és helyreállítás

Áttekintés

Előbb vagy utóbb mindannyiunkkal történik valami rossz, és ilyenkor elveszítjük a személyes fájljainkat, dokumentumainkat vagy fotóinkat. Véletlenül törölhetünk egyes állományokat, meghibásodhat a hardver, elveszíthetjük a mobil eszközt, vagy éppen vírustámadás áldozatává válhatunk. Amikor ilyen történik, gyakran a biztonsági másolatok segíthetnek abban, hogy helyreállítsuk a digitális életünket. Az OUCH! e havi kiadásában bemutatjuk, hogy mi az a biztonsági mentés, hogyan készítsük el azt, és hogy milyen mentési stratégiát alkalmazzunk saját részre.

A szerzőről

Heather Mahalik az iparban elismert biztonsági szakembernek számít, akinek az okostelefonok elemzése a fő területe. A Practical Mobile Forensics társszerzője, a Learning Android Forensics szerkesztője, valamint a FOR585 Advanced Smartphone Forensics és a FOR518 Macintosh Forensics SANS kurzusok társzerzője. Heather-ről a **Smarterforesnics.com** weboldalon és a **@heathermahalik** nevű Twitter csatornán tudhatunk meg többet.

Mikor és miről készítsünk biztonsági mentést?

A biztonsági mentés az adatainkról készült olyan másolat, amely valahol máshol van. Amikor elveszítjük fontos adatainkat, akkor ebből vissza tudjuk állítani azokat. A problémát az jelenti, hogy a legtöbb ember nem készít biztonsági másolatot, pedig rendkívül egyszerű és olcsó megoldás. Kétfajta megközelítés létezik: (1) csak a legfontosabb adatokról készítünk mentést, (2) minden fájlról - beleértve az operációs rendszert is - mentést készítünk. Az első megközelítés egyszerűsíti a mentés folyamatát, és tárkapacitást spórol meg számunkra. A második módszer viszont egyszerűbb és teljesebb körű megoldást ad. Ha nem vagyunk biztosak abban, hogy számunkra melyik a célravezetőbb, akkor a legjobb választás az, ha mindenről biztonsági mentést készítünk.

A következő lépésben meg kell határoznunk, hogy milyen gyakran akarunk mentést készíteni az adatainkról. A legelterjedtebb megoldás az óránkénti, napi vagy heti, stb. gyakoriságú mentés készítése. Az otthoni felhasználók számára rendelkezésre áll az Apple Time Machine vagy a Microsoft Windows Backup and Restore megoldása, amelyek segítségével automatikusan zajlik a folyamat, csak első alkalommal kell beállítani, utána akár el is felejthetjük. Ezek a megoldások csendben végzik a dolgukat, és a nap folyamán folyamatosan dolgoznak, miközben mi használjuk a számítógépet vagy éppen távol vagyunk. Más megoldások „folyamatos védelmet” ígérnek, ahol az új vagy éppen módosított fájlok azonnal biztonsági mentésre kerülnek, amint bezártuk azokat. Javasoljuk, hogy legalább naponta egyszer végezzünk biztonsági mentést. Végső esetben tegyük fel magunknak a kérdést: „Mennyi adatveszteséget engedhetek meg magamnak, hogy ha biztonsági mentésből kell helyreállítani a rendszert?”.

Biztonsági mentés és helyreállítás

Hogyan készítsük el?

Kétfajta lehetőség közül választhatunk: fizikailag létező adathordozóra vagy felhő alapú biztonsági mentést végzünk. A fizikailag létező adathordozó DVD lemezt, USB meghajtót, külső lemezt vagy más hasonló megoldást jelent. Bármelyik típusú adathordozót választjuk, a mentést soha ne arra az eszközre készüljön, amelyen az eredeti fájlok is vannak. A fizikai eszközök problémája az, hogy ha a helyszínt bármilyen káresemény éri (pl. tűz, lopás), akkor nem csak a számítógép semmisülhet meg, hanem a biztonsági mentést tartalmazó eszköz is. Ezért gondoljuk ki azt, hogy hol tudjuk biztonságosan, egy másik helyszínen elhelyezni a mentéseket hordozó tárolókat is, valamint gondoskodjuk arról, hogy azokon egyértelműen fel legyen tüntetve, hogy mit tartalmaznak, illetve mikor készültek. Az extra biztonság kedvéért akár titkosíthatjuk is az adathordozót.

Az automatizált, megbízható biztonsági mentések képzik gyakran az adatvédelem utolsó védelmi vonalát.

A felhő alapú megoldások teljesen másképp működnek. Ez egy olyan szolgáltatás, ahol a fájlokat valahol az Interneten tároljuk. A mentendő adatok mennyiségétől függően ez ingyenes vagy fizetős szolgáltatás is lehet. Úgy működik, hogy telepítünk egy programot a számítógépre, amely automatikusan menti a fájlokat a háttérben. Ennek a megoldásnak az az előnye, hogy bármilyen katasztrófa is történik a házunkkal, a felhőbe mentett adatok akkor is biztonságban vannak. Ezen kívül szinte bárhonnan, akár utazás közben is hozzáférünk a teljes biztonsági mentéshez vagy akár csak egyetlen fájlhoz. A hátránya az, hogy a mentés (és a helyreállítás szintén) lassabb, különösen, ha nagy mennyiségű adatról van szó. Ha nem tudunk dönteni, hogy melyik megoldás a számunkra legmegfelelőbb (fizikai adathordozóra vagy felhőbe mentsünk), akkor érdemes lehet mindkettőt igénybe venni.

Ne felejtsük el a mobil eszközöket sem! Az okos eszközök nagy előnye, hogy az adatok többsége már a felhőben van tárolva (email, naptárbejegyzések, telefonszámok és más kontaktinformációk). Azonban így is lehetnek olyan információk, amelyek nincsenek a felhőben tárolva (alkalmazások konfigurációs beállításai, a legújabb fotók vagy a rendszer információk). A mobil eszközről készített biztonsági mentés nem csak az információk megőrzésére szolgál, hanem segítségével könnyen és gyorsan helyre tudjuk állítani az eszközt akkor is, ha esetleg egy újabbra cseréljük a régit. Egy iPhone/iPad képes automatikusan menteni az Apple iCloud-ba. Az Android-nál és más típusú eszközöknél ez a gyártó vagy a szolgáltató beállításaitól függ. Bizonyos esetekben saját magunknak kell olyan alkalmazást vásárolnunk, amelyet kimondottan ilyen célra készítettek.

Helyreállítás

A biztonsági mentés elkészítése csak az út egyik fele. Meg kell győződnünk arról, hogy szükség esetén használni is tudjuk a mentést. Legalább havonta egyszer ellenőrizzük, hogy a biztonsági mentés működik (próbaképpen állítsunk helyre egy fájlt), és

Biztonsági mentés és helyreállítás

ellenőrizzük a tartalmát is. Ezen kívül készítsünk egy teljes mentést akkor is, ha a számítógépen, mobil eszközön rendszert akarunk frissíteni, vagy újat vásárolunk a régi helyett (vagy például egy új merevlemezt), és győződjünk meg arról is, hogy az használható.

Fontos lépések

- Automatizáljuk a biztonsági mentéseket és rendszeresen ellenőrizzük azokat!
- Amikor egy teljes rendszert kell helyreállítani biztonsági mentésből, mindig telepítsük a rendszerhez a legújabb biztonsági frissítéseket!
- Az elévült biztonsági mentéseket törölni kell, hogy illetéktelenek ne férhessenek hozzá!
- Ha felhő alapú megoldást használunk, nézzünk utána a szolgáltató irányelveinek és reputációjának, és győződjünk meg arról, hogy ezek megfelelnek az elvárásainknak! Például alkalmaznak-e titkosítást a tárolt adatokon? Ki férhet hozzá a mentésekhez? Támogatják-e az erős hitelesítési módszereket, mint például a két-faktoros hitelesítés?

További Információ

Iratkozzon fel a havi rendszerességű OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a http://www.securingthehuman.org weboldalon keresztül.

Magyar Kiadás

Kormányzati, távközlési és informatikai szolgáltatóként, Magyarország egyik stratégiai fontosságú gazdasági társasága a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Társaságunk kiemelt feladata a kormányzati infrastruktúra működtetése, az e-közigazgatási megoldások támogatása, valamint kormányzati szintű informatikai szolgáltatások nyújtása. További információ a http://www.nisz.hu oldalon olvasható.

Hivatkozások

A jelmondatokról:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_hu.pdf
Kétfaktoros hitelesítés:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201308_hu.pdf
A felhő biztonságos használata:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201409_hu.pdf
A titkosításról:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201408_hu.pdf

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Fordította: Birkás Bence, Árvai Gábor, Pál Benyó

