Havi biztonság tudatossági hírlevél mindenkinek

OUCH!

ebben a kiadásban...

- **Biztonsági mentések: Mit, Mikor és Hogyan**
- **Visszaállítás**
- **Főbb pontok**

Biztonsági mentés és helyreállítás

Áttekintés

Ha elég régóta használunk egy számítógépet vagy mobil eszközt, akkor előbb-utóbb történni fog valami rossz, ami miatt elveszíthetjük a személyes fájljainkat, dokumentumainkat vagy a fotóinkat. Például véletlenül rossz fájlt törlünk ki, hardverhibát észlelünk, elveszítjük az eszközünket, vagy megfertőződünk egy olyan malware-rel, mint a zsarolóvírus. Az ilyen esetekben gyakran a biztonsági mentés az egyetlen lehetőségünk, hogy visszaépítsük a digitális életünket. Ebben a hírlevélben elmagyarázzuk, mi is a biztonsági mentés, hogy készítsük biztonsági mentést az adatainkról és hogyan fejlesszünk ki egy olyan egyszerű stratégiát, ami megfelelő számunkra.

A szerzőről

Keith Palmgren, az IT biztonság területén szerzett több, mint 30 év tapasztalattal rendelkező Kiberbiztonsági szakember. Vezető SANS oktató, valamint a SANS SEC301 a „Bevezetés az információbiztonságba” kurzus szerzője. Keith sikeres tanácsadói tevékenységet folytat, a Twitteren elérhető: **@kpalmgren** néven.

Biztonsági mentések: Mit, Mikor és Hogyan

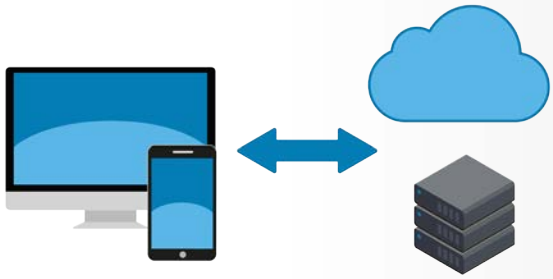
A Biztonsági mentések tulajdonképpen információk olyan másolatai, melyeket a számítógépünktől vagy mobil eszközünktől elkülönítve tárolunk. Amikor elveszítjük az értékes adatainkat, vissza tudjuk azokat állítani a biztonsági mentéseinkből. Sajnos sokan nem készítenek biztonsági mentéseket, annak ellenére, hogy ez egy egyszerű és olcsó megoldás. Első lépésként el kell döntenünk, hogy miről szeretnénk biztonsági mentést készíteni. Kétféle megközelítés létezik: (1) olyan különleges adatról, ami fontos nekünk, vagy (2) mindenről, beleértve a teljes operációs rendszerünket is. Számos biztonsági mentési megoldás úgy van beállítva, hogy alapértelmezettként az első megközelítést alkalmazza és a leggyakrabban használt mappáinkról készít biztonsági mentést. Sok esetben ez minden, amire szükségünk van. Ugyanakkor, ha nem vagyunk biztosak abban, hogy miről készítsünk biztonsági mentést, vagy rendkívül óvatosak akarunk lenni, akkor készítsünk mentést mindenről.

Másodszor el kell döntenünk, hogy milyen gyakran szeretnénk biztonsági mentést készíteni. A beépített biztonsági mentést készítő programok, mint az Apple Time Machine vagy a Microsoft Windows Biztonsági mentés és visszaállítás funkciója lehetővé teszik, hogy automatikus „állítsa be és feledkezzen meg róla” biztonsági mentés ütemezést állítsunk be. Gyakori lehetőségek az óránkénti, naponta, hetente stb. mentések. Más megoldások pedig „folyamatos védelmet” ajánlanak, mely keretében minden új vagy megváltozott fájlról készítenek egy biztonsági mentést, amint elmentünk egy dokumentumot. Legalább a napi rendszerességű biztonsági mentés ajánlott.

Végül el kell döntetnünk, hogy hogyan fogjuk a biztonsági mentéseket készíteni. Kétféleképpen készíthetünk biztonsági mentést az adatainkról: fizikai adathordozóra vagy felhő alapú tárhelyre. Mindegyik megközelítésnek megvannak az előnyei és hátrányai. Alkalmazható mindkét megközelítés is egyszerre, amennyiben bizonytalanok vagyunk abban, hogy melyik módszert válasszuk. Fizikai adathordozók például a külső USB meghajtó vagy a WiFi-vel elérhető hálózati

Biztonsági mentés és helyreállítás

eszközök. A saját fizikai adathordozó előnye, hogy nagyon gyorsan hozzáférhetünk a biztonsági mentésünkhöz és visszaállíthatunk nagy mennyiségű adatot. A hátránya ennek a megoldásnak, hogy ha olyan malware-rel fertőződünk meg, mint a zsarolóvírus, akkor elképzelhető, hogy a fertőzés átterjed a biztonsági mentéseinkre is. Egy katasztrófa - például tűz vagy lopás - esetén előfordulhat, hogy nem csak a számítógépünket veszítjük el, hanem a biztonsági mentéseinket is. Ha külső eszközöket használunk a biztonsági mentéseinkhez, akkor a biztonsági mentés egy másolatát az eszközünktől leválasztva, biztonságos helyen tároljuk. Figyeljünk rá, hogy a biztonsági mentéseket tároló adathordozókat megfelelően felcímkézzük.



Az automatizált, megbízható biztonsági mentések gyakran az utolsó védelmi vonalat jelentik az adataink megóvásában.

A felhő alapú megoldások olyan online szolgáltatások, melyek a fájljainkat az interneten helyezik el. Általában úgy működik, hogy feltelepítünk egy alkalmazást a számítógépünkre. Az alkalmazás ezután automatikusan elmenti a fájljainkat a magadott időzítés szerint, vagy az általunk végzett fájl módosítást követően. A felhőszolgáltatások előnye az egyszerűségükben rejlik, tekintve, hogy a biztonsági mentések általában automatikusak és a fájljainkhoz bármikor, bárhonnan hozzáférhetünk. Ha az adataink a felhőben találhatóak, az otthoni katasztrófák, mint például tűz vagy lopás, nem lesznek hatással a biztonsági mentéseikre. Végül a felhőben található biztonsági mentések segíthetnek nekünk, hogy visszaállítsuk a fertőzés előtti állapotot egy olyan malware fertőzés után, mint a zsarolóvírus. A hátránya, hogy hosszabb ideig tarthat a nagyobb mennyiségű adat mentése és visszaállítása. A személyes adatok védelme és biztonsága szintén fontos szempont. Bizonyosodjunk meg arról, hogy a szolgáltatás nyújt-e olyan erős, biztonsági funkciókat, mint például az adatok titkosítása és a kétfaktoros hitelesítés.

Végezetül ne feledkezzünk meg a mobil eszközeinkről sem. A mobil eszközeink esetében a legtöbb adatunk, mint például az e-mailek, naptáresemények, kontaktok már eleve a felhőben vannak eltárolva. Ugyanakkor a mobil applikáció beállításaink, legutóbbi fényképeink, rendszerbeállításaink nem kerülnek a felhőbe. A mobil eszközeinkről készített biztonsági mentéssel nem csak megőrizzük az információt, hanem új eszközre váltás esetén az adatok áthelyezése is könnyebb. Az iPhone/iPad automatikus mentést tud készíteni az Apple felhőbe. Az Androidos, illetve egyéb mobil eszközök esetében ez a gyártótól vagy a szolgáltatótól függ. Néhány esetben előfordulhat, hogy egy olyan mobil alkalmazást kell vásárolnunk, amelyet kifejezetten a biztonsági mentések készítésére hoztak létre.

Helyreállítás

Az adatainkról történő biztonsági mentés készítése csak fél siker, ugyanis biztosnak kell lennünk abban, hogy vissza is tudjuk állítani azokat. Időközönként ellenőrizzük le, hogy a biztonsági mentés működik-e, mégpedig úgy, hogy visszakeresünk egy fájlt és megállapítjuk, hogy megegyezik-e az eredetivel. Továbbá egy nagyobb rendszerfrissítés (például amikor egy gépről mobil eszközre vagy másik gépre váltunk) vagy jelentősebb javítás (mint például a merevlemez cseréje) előtt győződjünk meg arról, hogy készítettünk-e teljes rendszer mentést és ellenőrizzük, hogy az visszaállítható-e.

Biztonsági mentés és helyreállítás

Főbb pontok

- Attól függetlenül, hogy milyen megoldást választunk az adataink mentésére, bizonyosodjunk meg arról, hogy automatizáltuk-e a biztonsági mentés funkciót és időközönként ellenőrizzük is azt.
- Amikor visszaállítunk egy rendszert a biztonsági mentésből, bizonyosodjunk meg arról, hogy a legutóbbi biztonsági javításokat és frissítéseket használjuk.
- Kötelességünk megsemmisíteni az olyan elavult biztonsági mentéseket, amelyekre nincs többé szükségünk, ezzel is megakadályozva az illetéktelen személyek általi hozzáférést.
- Ha felhő szolgáltatást használunk, akkor a szolgáltató hírnevét és szabályzatait ellenőrizzük le és bizonyosodjunk meg arról, hogy megfelel-e az elvárásainknak. Például: titkosítják-e az adatainkat? Biztosítanak-e olyan erős hitelesítést, mint a kétlépcsős azonosítás?

További információ

Iratkozzon fel a havi OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a securingthehuman.sans.org/ouch/archives weboldalon.

Magyar Kiadás

A Nemzeti Kibervédelmi Intézet (NKI) látja el Magyarországon az állami és önkormányzati szervek vonatkozásában az elektronikus információbiztonsági hatósági, eseménykezelési, valamint a sérülékenység-vizsgálati feladatokat. A Nemzeti Kibervédelmi Intézet 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 http://www.govcert.hu/ és a http://neih.gov.hu oldalon olvasható.

Hivatkozások

Jelmondatok:	https://securingthehuman.sans.org/ouch/2017#april2017
Kétlépcsős azonosítás:	https://securingthehuman.sans.org/ouch/2015#september2015
Felhő biztonság:	https://securingthehuman.sans.org/ouch/2016#november2016
Titkosítás:	https://securingthehuman.sans.org/ouch/2016#june2016
Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016

Szerkesztette: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Fordította: Tikos Anita

