Biztonságos tárhelyet kínál a hazai Tresorit

Gálffy Csaba, 2013. április 10. 16:23 (http://www.hwsw.hu/)

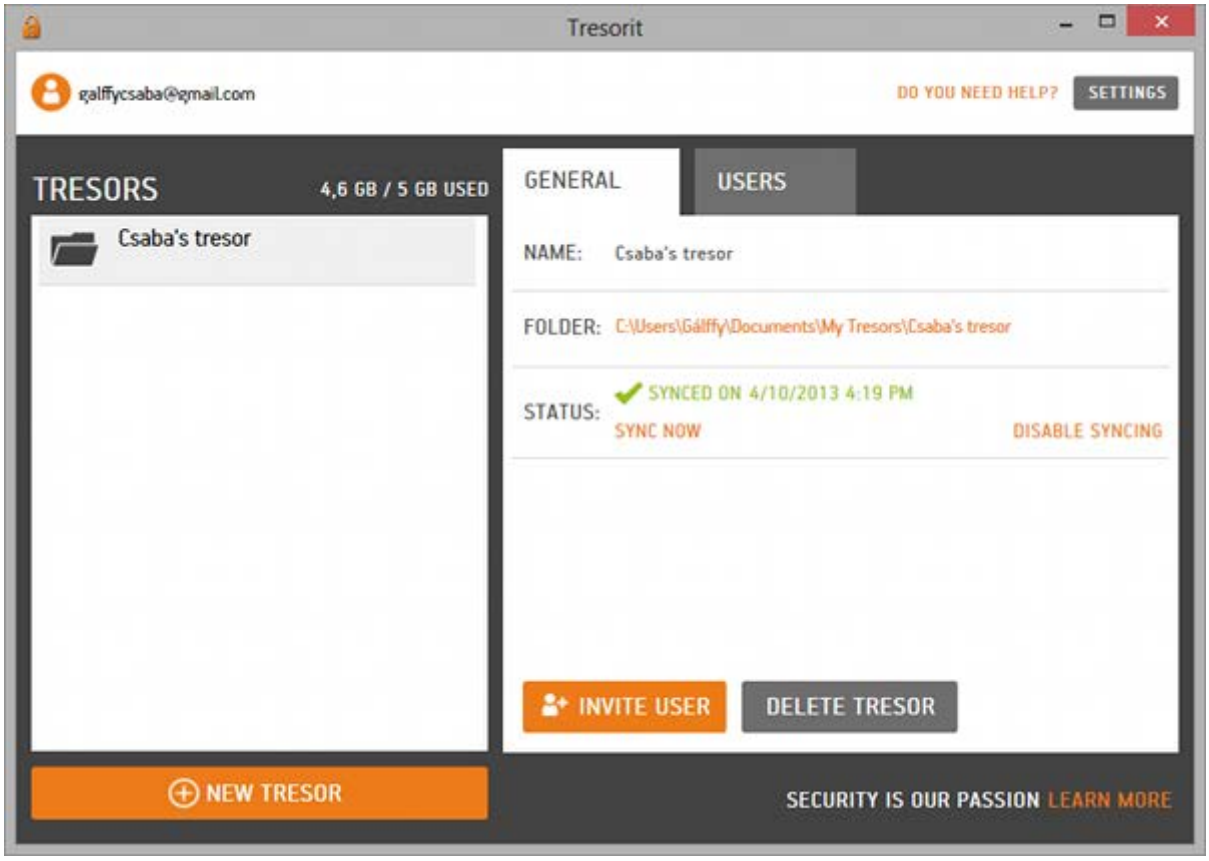
Kliensoldali titkosítással ellátott felhős fájlmegosztót mutatott be a hazai Tresorit. A startup két éve dolgozik annak megoldásán, hogy biztonságossá tegye ezt a szolgáltatást, az eredményt most bárki használatba veheti.

A közös munkavégzésben nagy előretörést hoztak a különböző fájlszinkronizációs szolgáltatások. Jó lemérhető ez például azon, hogy milyen eszközöket kezdenek a felhasználók saját hatáskörben "bevezetni" vállalati környezetben, saját munkájuk megkönnyítése érdekében. Ezek között élen jár a Dropbox és a hozzá hasonló felhős tárhelyek kategóriája, amelyek gyors fájlmegosztást és szinkronizációt biztosítanak az alkalmazottak és eszközeik között.

Bizalom-mentes működés

A felhős tárhelyek egyik legfontosabb problémája, hogy csak akkor tekinthetőek biztonságosnak, ha megbízunk a szolgáltatóban, a szolgáltató által használt infrastruktúrában és technológiában, valamint abban a jogi környezetben, amelynek szabályai a tárolt adatokra vonatkoznak. Lefordítva például a Dropbox példájára, a tárhely használatához mind a Dropboxban, mind az Amazonban, mind az amerikai szervekben meg kell bíznunk. A bizalom pedig nem csak arra vonatkozik, hogy maga a szolgáltató nem fog belenézni adatainkba, de arra is, hogy ő nem lesz támadás áldozata - ahogy tavaly nyáron fel is törték a rendszert.

A Tresorit-technológia lelke a kliensoldali titkosítás. A felhős tárhelyre feltöltött fájlokat feltöltés közben titkosítja a rendszer, a tárolóra pedig az állományok kódolt formában érkeznek. Ezzel kiküszöbölhető, hogy a tárolt adatokhoz a kulcs nélkül bárki hozzáférjen, legyen az akár a tárhely, akár a szolgáltatás üzemeltetője. A megközelítés logikus hátulütője, hogy a kulcs elvesztése esetén az adat tulajdonosa sem fér hozzá a tárolt információkhoz, ebben segítséget pedig a szolgáltató sem tud adni. Ezen a téren némi változást a nagyvállalati, fizetős megoldás hoz majd, ilyen környezetben elérhető lesz egy alternatív escrow-kulcs is, amellyel az egyes alkalmazottak fiókjai nyithatóak maradnak. Okos biztonsági megfontolás, hogy a mindent nyitó kulcsnak csak a részeit kapják meg a vezetők (vagy a rendszergazdák), így egymás tudta nélkül ők sem férnek hozzá a tárolt adatokhoz.



Egyszerű, letisztult felület, pofonegyszerű használat.

A cég képviselői szerint a Dropbox és hasonló rendszerek ma is használhatóak biztonságos módon, ha helyben titkosított fájlokat töltünk fel, a kulcsot pedig megosztjuk azokkal, akikkel az állományt is. Erre például a PGP kiválóan alkalmas - lenne. Az ilyen rendszerek használata ugyanis roppant körülményes, esélytelen, hogy ezt egy nem műszaki képzettségű irodai csoport napi szinten használni kezdje. A Tresorit pontosan ezt a piaci rést szeretné betömni, az alapértelmezetten biztonságos, ám egyszerű alkalmazás megtanulása nem nehéz. A startupnál egyébként a munkaerő egyharmada dolgozik a felhasználói élményen, a UX-en, ennyire fontos ez a szempont a fejlesztésben.

A Tresorit jelenleg béta állapotban érhető el, a cég oldaláról a kliensszoftvert letöltve regisztrálhatunk egy 5 gigabájtos ingyenes fiókot. A kiterjesztett vállalati funkciók és a fizetős szolgáltatások később válnak elérhetővé, egyelőre az alaprendszert teszteli a cég - ennek megfelelően minden visszajelzést igyekeznek beépíteni a termékbe. A tervek közt szerepel egy menedzsment-felület is, amellyel a nagyobb vállalatok is könnyen implementálhatják és üzemeltethetik a rendszert.
Ez azt jelenti, hogy a Dropboxszal ellentétben a Tresorit esetében csak a titkosítási technológiában kell megbíznunk, a támadók hiába férnek hozzá ezután bármilyen adatunkhoz, a titkosított állományok tartalma teljes biztonságban marad. A cég képviselői szerint az adatvédelem a feltöltött fájlokra vonatkozik, a feltöltő egyes adatai (email-címe, számlázási címe, neve és IP-címe) ismert a Tresorit számára, és elméletileg támadók által is megszerezhető, illetve arra jogosult hivatalos szervek is kikérhetik ezeket az információkat.

Fókuszált szolgáltatás

A Tresorit-technológia másik korlátja, hogy a PC-n helyben tárolt adatokat nem védi titkosítás. Ez tudatos döntés eredménye, az operációs rendszerek jellemzően erős lemeztitkosítással rendelkeznek, amennyiben erre van igény, akkor ennek bekapcsolását javasolja a cég. A döntés logikus, egy ilyen rendszer független, biztonságos implementációját kifejleszteni fantasztikus erőfeszítés lenne, ráadásul felesleges is, mivel a legtöbb asztali operációs rendszer rendelkezik erre beépített megoldással.

Az on-the-fly, feltöltés és letöltés közbeni titkosítást és visszafejtést végző kód C++-ban íródott, mivel ez számít a leghordozhatóbbnak a különböző platformok között. A Tresorit képviselői szerint az algoritmus gyakorlatilag módosítás nélkül fut Windowson és Windows Phone-on, OS X-en, Androidon (Java Native Interface használatával) és az Objective-C-kompatibilitás révén az iOS is lefedett. A különböző platformokhoz természetesen szükséges natív felületek készítése, de maga titkosítási technológia lehet egységes. A közös kódbázis hatalmas előnye, hogy a folyamatos fejlesztések is folyhatnak a közös ágon és az eredmények azonnal megjelennek a kliensekben.

Ez is startup

A Tresorit tavaly nyáron vont be első körben kockázati tőkét, akkor 380 millió forintért szerzett a cégben részesedést az Euroventures és kilenc magánszemély. A Tresoritot egyébként 2011-ben alapította a BME három informatikus hallgatója, Buttyán Leventével, a BME CrySys labor tagjával együtt. Azóta volt némi helycsere, közben pedig mintegy 20 főre bővült a szolgáltatás fejlesztésével foglalkozó csapat létszáma. A Tresorit tárolóbackendjét egyébként a Microsoft Azure infrastruktúra-szolgáltatása adja. Lám István, a cég ügyvezetője elmondta, hogy egyelőre egy Microsoft BizSpark Plus ösztöndíjat elnyerve ingyen használhatják a szolgáltatást.

A rendszer biztonságát hirdetendő a cég 10 ezer dolláros jutalmat ígér annak, akinek sikerül hozzáférnie egy elkülönített szerveren tárolt szimulált ügyféladatokhoz. Lám István, a Tresorit ügyvezetője a HWSW kérdésére elmondta, hogy nem véletlenül esett a választás a tízezer dolláros összegre, ekkora "vérdíjat" tűzött ki magára a Mega, Kim Dotkom új online tárhelyszolgáltatása is. A Mega azonban komoly korlátokat állít a támadók elé, nem csak a fájltitkosítást, de a szervert is fel kell törni az adatok megszerzéséhez, a Tresorit esetében a szerver nyitott, csak a saját titkosítást kell megtörni.

"Úgy gondoljuk, hogy egy olyan rendszert sikerült létrehoznunk, hogy mi, mint szolgáltatók sem férnénk hozzá a tárolt adatokhoz" - mondta Lám. "Ezt bizonyítani akarjuk, ezért a verseny külön szerverén a hackerek a szimulált felhasználók adatait ugyanolyan formában tekinthetik meg, mint maguk a Tresorit rendszergazdái." A kihívás április 15 után lép életbe, az első eredményeket pedig a május 9-én, az Ethical Hacking biztonsági konferencia keretében hozza nyilvánosságra a Tresorit.