

Fizikai adatvédelem: Titkosítás 5 perc alatt!

Ptk. 81. § (2) definiálja az üzleti titok fogalmát. A könyvvizsgáló a munkája során nem csak a személyes titoktartásra kötelezett, hanem felelős azoknak az eszközöknek használatáért is, amelyeket a munkájához rendszeresít. A könyvvizsgálat napi munkája során az informatikai eszközök alkalmazása már elengedhetetlen, így a programok, alkalmazások használatakor keletkezett adatok, információk, kimutatások, saját vélemények, a megbízó által átadott elektronikus anyagok és egyéb dokumentumok jogosulatlan hozzáférésből eredő érdeksérelmének a kockázata is jelentősen megnőtt.

Az információ-védelem három terület kezelését emeli ki: Informatikai eszközvédelem, alkalmazásvédelem és az adatvédelem. Ezek a kategóriák biztonsági szempontból klasszikusan elkülönülten kezelendők. Napjainkban viszont a legkritikusabb terület az adatvédelem, aminek egyik oka az adatvagyon kritikus méreteket öltő növekedése.

Egyre inkább teret hódít, és a jövő munkamódszere az informatikai eszközök csoportmunkában történő használata. Ekkor viszont jelentősen megnövekszik a közös adattárak biztonságos használatának a kockázata. Az így kialakított környezetben kihívásként fogalmazódik meg az egyedi alkalmazások rugalmassága, és a hordozhatósága. Ez igényli az igényeknek megfelelő új eszközök bevezetését.

Az elvárás:

Az, hogy az adatvédelem és az adatbiztonság érdekében a saját dokumentumainkat elkülönítetten, jelszóval védetten egy külön könyvtárban helyezzük el úgy, hogy a könyvtár csatolása, megnyitása csak a jelszó megadásával legyen lehetséges. Viszont: Az éppen futtatott alkalmazás ne érzékelje azt, hogy védett eszközön elhelyezett dokumentummal, adatállománnyal dolgozik.

A megoldás:

Több megoldási lehetőség is alkalmazható a gyakorlatban. A legegyszerűbb, legnépszerűbb és az elvárásoknak leginkább megfelelő a **TrueCrypt** szabad szoftver, ami egy valósidejű titkosítást megvalósító *ingyenes, nyílt forráskódú titkosító szoftver*.

Ennek segítségével a titkosított adatokat egyetlen file-ban lehet tárolni - szinte bármilyen adathordozón. Később pedig ez úgy használható, mint egy külön partíció.

A böngészőn keresztül a file kiválasztásával történik a tartalom csatolása (és a betű hozzárendelése). A jelszó megadása is a kiválasztáskor történik, és azt a rendszer a lecsatolásig megjegyzi. Ez a megoldás lehetőséget biztosít egy egész partíció, illetve meghajtó titkossá tételére is. (Ennek méretét - a titkosítandó adattartalomhoz igazítottan - mindig a felhasználó szabja meg.)

Maga az eljárás az alkalmazáskor saját file-rendszert használ - ami szintén titkosítva van.

A megoldás további előnye, hogy a Microsoft Windows, Linux és Mac OS X operációs rendszereken működik ugyanúgy működik az alkalmazás. Az Ms. Office Word vagy Excel dokumentuma a Linux rendszerben futó Open Office Writer illetve Calc alkalmazásokkal gond nélkül megnyithatók. Rugalmas, mert a különböző rendszerekben mentett file-ok az alkalmazáson keresztül kezelhetők.

Külső adatszerveren (vagy a felhőben) is elhelyezhető a titkosított file, és annak csatolása ugyanúgy történik, mintha azt a saját géphez csatlakoztatott adattároló eszközön végeznénk.

További információ: [Wikipédia](#)

Kapcsolódó anyagok: https://www.mkvk.hu/szervezet/tagozatok/IT_tagozat/TagozatiHirek/TrueCrypt-5perc-alatt.htm

Telepítő alkalmazások [TrueCrypt_Setup_6.1a.exe](#) [TrueCrypt_en_7.0a.exe](#)