

Bár az elmúlt években egy kicsit eltávolodtam az informatikai biztonsági feladatoktól, most mégis vissza kellett zökkennem erre a területre egy apró feladat erejéig.

Úgy gondolom tanulságos volt. Muszáj elsütnöm azt a hangzatos közhelyt miszerint a notebookon tárolt adatok gyakran értékesebbek a tulajdonosa számára mint maga a gép. Ezért aztán védeni kell őket, hogy elvesztés, ellopás esetén se kerülhessenek illetéktelen kezekbe.

A feladat megoldására

három "versenyzőt" választottam ki amelyek egyaránt képesek a merevlemez teljes titkosítására.

Az egyik hamar kiesett mivel a Microsoft Bitlocker funkcióját

csak a Windows 7 Ultimate és Enterprise verziói tartalmazzák. A cél gépen viszont csak a Windows 7 Home x64 változata volt. Így csak két induló maradt versenyben a Safeguard Easy és a ProtectDrive.

Beszereztem mindkét programhoz 1-1 próba változatot. A Safeguard 30 napos változata letölthető a gyártó weblapjáról míg a ProtectDrive próbaverzióját a forgalmazótól szereztem be. A tesztkörnyezet VMWare 7-es virtuális gép, úgy gondolom ma már ez természetes még ha egy olyan hardware közeli alkalmazást is tesztelünk mint a merevlemez titkosítás. A Safeguard meggyőzően teljesített, telepítése igen egyszerű volt és tökéletesen működött a virtuális környezetben.

Ezeknek az alkalmazásoknak tömören az lényege, hogy a Windows helyett a titkosító alkalmazás indul el a gép bekapcsolásakor és kéri be a felhasználó nevet és jelszót. Ha ez helyes akkor visszatitkosítja a file rendszert és engedi elindulni a Windowst. Bár ez így nagyon le van egyszerűsítve de a lényeg mégis csak ez. Tehát a Safeguard esetében mindez remekül működött, csak azt hiányoltam hogy szinte semmi beállítási lehetőséget nem kínál a program, de ezt a próbaverzióknak tudtam be. A ProtectDrive esetében viszont más volt a helyzet, a program lényegesen testre szabhatóbb, részletesen beállítható hogy melyik belső vagy külső lemezt titkosítsa,

mit tegyen a

pendrive-al, CD/DVD lemezzel, stb, stb..

A gond csak ott kezdődött, hogy bár a

telepítés utáni újraindításkor ugyan bekérte a felhasználónevet és jelszót de a Windows ezután nem indult el, bár egy pillanatra felvillant egy "Windows now booting" üzenet de utána csak fekete képernyő és

más semmi. Megpróbáltam újratelepíteni de ugyanez történt. Aztán ráuntam a dologra és ott hagytam a gépet. Mikor visszatértem csodálkozva láttam, hogy elindult a Windows és működik is kifogástalanul, csak hát minden indításkor kb 20 perc kellett neki hogy betöltsön.

Mivel már így is túl sok időt töltöttem az ügygel ezért a választás a SafeGuard-ra esett és vásároltunk egy azaz egy darab licencet. A SafeNet-et a ProtectDrive tulajdonosát annyira megrázta ez a hír hogy azóta többször is telefonon érdeklődtek döntésünk okáról valahonnan Spanyolországból.

Ez már a globalizáció azt hiszem.

Safeguard

A Safeguard mostanában jelentős átalakuláson megy át, a Sophos felvásárolta a korábbi fejlesztő céget az Utimaco-t. Talán ennek tudható be, hogy a letölthető próbaváltozat köszönő viszonyban sincs a jelenleg forgalmazott termékkel. Sajnos! Ugyanis az egy gépre telepíthető (alias: standalone) változat bizonyos mértékben kimúlt. A szoftver egyetlen gépes használata esetén is fel kell valahova telepíteni a Safeguard policy editorát (.NET framework-el, MSDE-adatbázissal, hálózati megosztásokkal, Brrrrr....)

hogy egy konfigurációs állományt készíthessünk .MSI csomag formájában. Nos ez egy szép kis feladat, főleg ha az ember úgy gondolta előtte hogy az egész telepítést majd letudja egy óra alatt. A Safeguard filozófiája elég egyértelmű, semmit se bízni a felhasználóra, keményen kikényszeríteni minden szabályt a felhasználó megkérdezése nélkül. Én ezt meg is értem, egy nagyvállalat esetében ennek abszolút van létjogosultsága. Jelen esetben viszont egy kicsit nagyobb szabadságot szerettem volna adni a notebook tulajdonosának, miszerint a csatlakoztatott külső eszközökről (merevlemez, pendrive) ő dönthesse el, hogy titkosítva legyenek-e vagy sem. Tehát kicsit sarkosnak érzem azt a megoldást amit Safeguard kínál miszerint vagy minden külső eszközt kérdés nélkül titkosít vagy semmit.

Mindezekért cserébe viszont a Safeguard

valóban észrevétlenül és gyorsan teszi a dolgát, teljesítmény csökkenést szinte nem is okozva.

Időt csak a merevlemezek első titkosítására kell szánni mert a lemez méretétől függően ez súlyos órákba telik, viszont

ez igaz a konkurens termékekre is.

ProtectDrive

Akadtak gondjai a VMWare-es tesztkörnyezettel mert indítás és jelszóbekérés után kb. 20 percbe telt minden alkalommal míg a Windows elindult, de tudjuk ezt be a virtuális gépnek. A ProtectDrive működése szinte teljesen megegyezik a Safeguard-al így inkább csak a különbségeket taglalnám. A P.D. sokkal egyszerűbben testre szabhatóbb, nincs szükség Policy Editor-ra mert a felhasználó szabadon állíthatja be melyik merevlemez kívánja titkosítani. Ez jóval nagyobb szabadságot jelent a SG-hoz képest. Persze a ProtectDrive-nak is van vállalati környezetbe Active Directory-ba integrált változata, de a teszt most csak egy gépes környezetre terjedt ki. Biztos, hogy a három vizsgált termék közül a Protect Drive kínálja a legrészletesebb beállítási lehetőségeket. Beállíthatjuk hogy mely felhasználók jelentkezhetnek be egyáltalán a gépünkre, hogy bejelentkezés után milyen üzenetek jelenjenek meg (Pl. hogy ki és mikor lépett be utoljára a gépünkre), milyen algoritmusokat használjon a program a titkosításra, az egyes felhasználók milyen eszközökre írhatnak vagy olvashatnak, stb..

A tesztben a rendszer merevlemezen kívül egy 8 GB-os pendrive-ot is titkosítottam mely kb. 35 percig tartott amit mindenképp sokallok. De el kell ismerni, hogy a kezdeti titkosítás mind három versenyzőnél nagyon sokáig tart. A titkosított pendrive viszont más rendszeren nem olvasható, ez mindenképp hátrány.

BitLocker

Mint utaltam már rá korábban, a Microsoft BitLocker-e csak a Windows 7 Ultimate és Enterprise változatainak része, az árkülönbség viszont nem olyan óriási. A Windows 7 Home változatainál kb. 20e, míg a Professional változataihoz képest kb. 15e forinttal több. Ha a Windows vásárlásakor már tudjuk, hogy szükségünk lesz merevlemez titkosításra válasszuk ezt, bizonyosan ez a leggazdaságosabb megoldás és ráadásul jó is! Viszont vannak itt hardware követelmények melyeket figyelembe kell venni.

Ahhoz, hogy az operációs rendszer partícióját is titkosítani tudjuk a gépnek rendelkeznie kell TPM modullal. Leegyszerűsítve ez egy kis chip ahol a titkosításhoz használt kulcsot tárolja a rendszer.

A TPM modul nem ritkaság, ma már nagyon sok, elsősorban üzleti célú notebook van forgalomban ami tartalmazza ezt. De ha nincs TPM a gépünkben akkor sem vesztett minden. Particionáljuk kétfelé merevlemezünket. Az egyik felére (jellemzően C: meghajtó) telepítsük a Windowst és lehetőség szerint ne tároljunk rajta semmi értékes adatot. A második partíciót (jellemzően D: meghajtó) viszont már nyugodtan titkosíthatjuk a BitLocker-el. Ennek eredményeképpen minden Windows indítás után amikor először akarunk adatot olvasni/írni a titkosított meghajtóról a BitLocker bekéri az eléréshez szükséges jelszót. Tehát hiába lopják el gépünket, és hiába tudják esetleg elindítani a Windows-t a titkosított adatainkhoz a jelszó hiányában akkor is lehetetlen hozzáférni. A hordozható eszközeink (Pendrive) védelmére pedig ott a "Bitlocker To Go" mely titkosítást bármely windows 7 kliens képes kezelni, míg a korábbi windows verziók részére kapunk egy kliens programot melynek segítségével képesek leszünk olvasni a pendrive-ról de írni nem fogunk tudni rá.

Konklúzió:

A legegyszerűbb és legolcsóbb megoldás a Windows7 BitLockere. Különösen akkor ha előre tudunk tervezni és már vásárláskor a megfelelő Windows7 verziót és TPM chipes notebook-ot választunk. Nagyvállalati környezetben a SafeGuard is jó választás lehet, sok gép esetén megéri a fáradságot elkészíteni a megfelelő policy-t mely szigorúan őrökdi adataink biztonságán. A ProtectDrive jó választás lehet ha Windows-unk nem támogatja a Bitlocker-t és egy egyszerű de nagy tudású alkalmazást szeretnénk.