DIGITÁLIS KÁRTEVŐK & BIZTONSÁGI MENTÉS

A számítógépek és mobileszközök internetre történő csatlakozása jelentősen megkönnyíti a számítógépes vírusok és más rosszindulatú szoftverek elterjedését. 2017-ben 4,2 másodpercenként jött létre egy új digitális kártevő, ami azt jelenti, hogy csak a tavalyi évben több mint 7,5 millió új vírust és más rosszindulatú szoftvert készítettek, valamint több mint 72 millió weboldal volt fertőzött. Éves szinten több mint 10 milliárd USD kárt okoznak a rosszindulatú programok.

ROSSZINDULATÚ SZOFTVEREK

A rosszindulatú szoftverek a vírusok, férgek, kémprogramok, agresszív reklámprogramok és a rendszerben láthatatlanul megbúvó, a támadónak emelt jogokat biztosító eszközök összefoglaló neve.
A rosszindulatú programok célja lehet:

- a számítógép vagy eszköz tönkretétele,
- fájlok, adatok módosítása vagy törlése,
- a megfertőzött számítógép internetkapcsolatának használata illegális célokra (pl. spam küldésére),
- zsarolás a fájlok titkosításával,
- a felhasználó jelszavainak, bankkártya adatainak megszerzése.

A vírusok manapság jellemzően pendrive vagy e-mail segítségével terjednek az internetes böngészés (a megbízhatatlan oldalakról történő letöltések) mellett. Számítógépes értelemben a trójai faló (röviden trójai) egy olyan rosszindulatú program, ami mást tesz a háttérben, mint amit a felhasználónak mutat. Ebben az esetben a leggyakoribb fertőzési módszert az ingyenes vagy nem jogtiszta programok letöltése és a veszélyes honlapok jelentik.

VÉDEKEZÉS LEHETŐSÉGEI

A rosszindulatú szoftverek a számítógép operációs rendszerének és egyéb programjainak biztonsági hibáit használják ki. A szoftverek gyártói az ismertté vált hibákat rendszeresen javítják és frissítések kiadásával juttatják el a felhasználókhoz. A frissítések kiadásával az addig esetleg nem nyilvános hibákról is tudomást szerezhetnek a rosszindulatú szoftvereket készítők, így azok a rendszerek, amelyeken a hibákat javító frissítés nem történt meg, fokozattan veszélyeztetettek lehetnek.
A kártékony programok elleni védekezés céljából feltétlenül javasolt vírusirtó program telepítése, amelyek elérhetőek ingyenes és fizetős változatban is.
A tűzfal célja a privát (otthoni/vállalati) és nyilvános (internet) hálózat elkülönítése, továbbá annak biztosítása, hogy a hálózaton keresztül egy adott számítógépbe ne történhessen illetéktelen behatolás. Amennyiben a számítógép közvetlenül kapcsolódik az internethez, szoftveres tűzfal használata javasolt. Ha az internetelérés routeren keresztül történik, akkor az általában tartalmaz tűzfalat. Ebben az esetben győződjünk meg róla, hogy be van-e kapcsolva!

BIZTONSÁGI MENTÉS

Rendszeresen készítsünk biztonsági másolatot fontos adatainkról.
Erre alkalmas lehet egy külső merevlemez, amit csak a biztonsági mentés idejére csatlakoztatunk a számítógéphez vagy egy online tárhely, ahol a fájlok korábbi verzióját tároljuk. Így ha zsarolóvírus-támadás éri a gépet, a rosszindulatú program eltávolítását követően az ép verziók visszaállíthatóak.

- Javasolt az automatikus frissítés bekapcsolása.
- Állítsuk be, hogy a kritikus műveletekhez (pl. program telepítése) a felhasználó engedélyére legyen szükség.
- A böngészők biztonsági beállításainál a magasabb védelmi szint a külső támadások ellen nyújt védelmet.
- Ismeretlen eredetű szoftvereket ne telepítsünk!
- Telepítsünk a gépre vírusirtó programot, amely legyen mindig aktív!
- Rendszeresen készítsünk biztonsági másolatot a fontos adatainkról!