

# 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 7,5 millió új vírus 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.

#DIGITÁLISKÁRTEVŐ

#VÍRUS

#TŰZFAL

#BIZTONSÁGI MENTÉS

#ONLINE TÁRHELY

## ROSSZINDULATÚ SZOFTVEREK

A rosszindulatú szoftverek (angolul malware: malicious software összevonás) 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 küldésre),
- 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 oldalokról történő letöltések) mellett. Számítógépes értelemben a trójai faló (röviden trójai) egy olyan rosszindulatú program, ami mást tesz a háttérben, mint amit a felhasználónak mutat. A trójaiak esetében leggyakoribb fertőzési módszert az ingyenes vagy nem jogtisztá programok letöltése és a veszélyes honlapok jelentik.

## A VÉDEKEZÉS LEHETŐSÉGEI

A rosszindulatú szoftverek a számítógépen futó szoftverek (operációs rendszerének és egyéb programok) biztonsági hibáit használják ki. A szoftverek gyártói az ismertté vált hibákat rendszeresen javítják, és frissítések kiadásával juttatják el a felhasználókhöz. A frissítések

kiadásával az addig esetleg nem nyilvános hibákról is tudomást szerezhetnek a rosszindulatú szoftvereket készítő, így azok a rendszerek, amelyeken a hibákat javító frissítés nem történt meg fokozatosan veszélyeztetettek lettek.

A vírusok (és egyéb kártékony programok) elleni védekezés céljából feltétlenül javasolt vírusirtó program telepítése, amelyek elérhetőek ingyenes és fizetős változatban is.

A tűzfal (angolul firewall) 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 internetelés routeren keresztül történik, akkor az általában tartalmaz tűzfalat. Ebben az esetben győződjünk meg róla, hogy az be van kapcsolva!

## BIZTONSÁGI TANÁCSOK

- Frissítések telepítése érdekében javasolt az automatikus frissítés bekapcsolása.
- Felhasználói fiókok felügyeletén állítsa be, hogy a kritikus műveletekhez (pl. program telepítése) felhasználó engedélyére legyen szükség.
- Böngészők biztonsági beállításai: a magasabb védelmi szint a külső támadások ellen nyújt védelmet.
- Ismeretlen eredetű szoftvereket ne telepítsen!
- Telepítsünk vírusirtó programot a gépre, és ne kapcsolja ki!
- Rendszeresen készítsen a biztonsági másolatot a fontos adatainkról!

# INTERNET TUDATOSAN

## ONLINE IS BIZTONSÁGBAN

### BIZTONSÁGI MENTÉS

Rendszeresen készítünk biztonsági másolatot fontos adatainkról.

Erre alkalmas lehet egy külső merevlemez, amit csak a biztonsági mentés idejére csatlakoztatunk a számítógéphez vagy olyan online tárhely, amely tárolja a fájlok korábbi verzióját.

Online tárhely esetében azért fontos a fájl verziók korábbi eltárolása, mert, ha zsarolóvírus támadás éri a gépet, akkor az automatikus szinkronizációnak köszönhetően a titkosított fájlok kerülnek az online tárhelyre is, de a vírus eltávolítását követően a legutolsó ép verziók visszaállíthatóak.