# 3. 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 abban az évben több mint 7,5 millió új vírus és más rosszindulatú szoftvert készítettek, és több mint 72 millió weboldal fertőződött meg. Éves szinten több mint 10 milliárd USD kárt okoznak a rosszindulatú programok.

## ROSSZINDULATÚ SZOFTVEREK

A **ROSSZINDULATÚ SZOFTVEREK** (angolul malware: malicious software összevonása) a vírusok, férgek, kémprogramok, agresszív reklámprogramok és a rendszerben láthatatlanul megbúvó, a támadónak emelt jogokat biztosító eszközök (rootkit) összefoglaló neve.

A rosszindulatú programok célja lehet:

- a számítógép vagy eszköz **TÖNKRETÉTELE**,
- fájlok, adatok **MÓDOSÍTÁSA VAGY TÖRLÉSE**,
- a megfertőzött számítógép **INTERNET-KAPCSOLATÁNAK 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 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. A trójaik esetében leggyakoribb fertőzési módszert az ingyenes vagy nem jogtiszta programok letöltése és a fertőzött honlapok jelentik.

## 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!
- Telepítsen **VÍRUSIRTÓ** programot a gépre, és ne kapcsolja ki!
- Rendszeresen készítsen **BIZTONSÁGI MÁSOLATOT** a fontos adataikról!

## A VÉDEKEZÉS LEHETŐSÉGEI

A rosszindulatú szoftverek a számítógépen futó programok (operációs rendszer és egyéb programok) **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

# KIBERBIZTONSÁGI TIPPEK

nyilvános hibákról is tudomást szerezhetnek a rosszindulatú szoftvereket készítők, így azok a rendszerek, amelyeken a hibákat javító frissítés nem történt meg **FOKOZATTAN VESZÉLYEZTETTEK** 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 a 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 győződön meg róla, hogy az be van kapcsolva!

## BIZTONSÁGI MENTÉS

Rendszeresen készítsen **BIZTONSÁGI MÁSOLATOT** fontos adatairól!

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 korábbi **FÁJLVERZIÓK** eltárolása, mert ha zsarolóvírus-támadás éri a gépet, akkor az automatikus szinkronizációnak köszönhetően a titkosított fájlok kerülhetnek az online tárhelyre is, de a vírus eltávolítását követően a legutolsó ép verziók **VISSZAÁLLÍTHATÓAK**.

**TOVÁBBI INFORMÁCIÓK ÉRHETŐEK EL AZ ALÁBBI LINKEKEN**

www.police.hu/hu/hirek-es-informaciok/bunmegelozes/internet-biztonsag

www.facebook.com/internettudatosan

INTERNET ONLINE IS BIZTONSÁGBAN TUDATOSAN

Országos Rendőr-főkapitányság