# SZÁMÍTÓGÉPÜNK VÉDELME

Az internet használata során számos veszély fenyegeti a felhasználókat és számítógépeiket. Ezekkel szemben a megfelelő biztonsági intézkedésekkel és magatartási szabályok tudatos betartásával lehet védekezni. Az aktuális kiadványunkban ezeket a veszélyeket és az ellenük való védekezés módjait mutatjuk be.

## A SZÁMÍTÓGÉP MEGFELELŐ BEÁLLÍTÁSA

A rosszindulatú szoftverek és hackerek a számítógépen futó operációs rendszer és egyéb programok biztonsági hibáit használják ki. A szoftverek gyártói az ismertté vált hibákat rendszeresen javítják, és a javításokat frissítések kiadásával juttatják el a felhasználókhoz. Az operációs rendszer automatikus biztonsági frissítésének bekapcsolásával biztosítható, hogy a számítógép a frissítés közzétételét követő legrövidebb időn belül megkapja azokat. A felhasználói programok jelentős része szintén jelzi, hogy újabb verzió elérhető, ezek telepítése is ajánlott.

## VÍRUSIRTÓ PROGRAMOK

A vírusok (és egyéb kártékony programok) elleni védekezés céljából feltétlenül javasolt vírusirtó program telepítése.

- A hagyományos vírusirtó programok adatbázisok alapján azonosítják a káros programokat. Az adatbázist a vírusirtó szoftver gyártója rendszeresen frissíti, a frissítéseket a legtöbb vírusirtó szoftver automatikusan letölti az interneten keresztül. Ez a reaktív védelem.
- A modern vírusírtó programok beépített elemző algoritmusok segítségével – a programok kódjának elemzésével – azonosítják a vírusokat (heurisztikus védelem). Mivel egy új vírus megjelenése után több nap is eltelhet, amíg a vírusirtó program gyártója adatbázisát frissíti, addig a reaktív vírusírtó nem nyújt védelmet. A heurisztikus módszereket is alkalmazó modern vírusirtók viszont addig is védelmet nyújtanak a legtöbb kártevő ellen, amíg a frissítés megtörténik.

## TŰZFAL

A tűzfal 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.

- **Hardveres tűzfal:** valamilyen fizikai eszköz, ami a privát és a nyilvános hálózat között monitorozza és szabályozza a bejövő és kimenő hálózati forgalmat a beállított tűzfal szabályoknak megfelelően. Korlátozott tűzfalként alkalmazható egy otthoni router is, amely megfelelően beállítva kellő védelmet nyújthat a külső támadások ellen.
- **Szoftveres tűzfal:** a tűzfal-szoftver a számítógépen fut (pl. Windows beépített tűzfala), és a számítógép bejövő és kimenő hálózati forgalmát monitorozza és szabályozza. Alkalmazása akkor indokolt különösen, ha a számítógép közvetlenül – nem routeren keresztül – csatlakozik az internethez.

## BIZTONSÁGI MENTÉS

Rendszeresen készítsünk 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 tárolása, mert ha egy zsarolóvírus megtámadja 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.

## JAVASLATOK

- Frissítések telepítése érdekében javasolt az automatikus frissítés bekapcsolása.
- Felhasználói fiókok felügyeletén állítsuk be, hogy a kritikus műveletekhez (pl. program telepítése) a felhasználó engedélyére legyen szükség.
- Állítsuk magasabb szintre a böngészők biztonsági beállításait!
- Ismeretlen eredetű szoftvereket ne telepítsünk!
- Csak ismerős feladó által küldött e-mail mellékletét nyissuk meg!
- Ne adjunk meg jelszót, PIN kódot e-mailben küldött kérésre!
- Ne adjuk meg senkinek felhasználói nevünket és jelszavunkat!