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.

#AutomatikusFrissítés #RosszindulatúSzoftverek #Vírusirtó #Tűzfal #BiztonságiMentés

A SZÁMÍTÓGÉP MEGFELELŐ BEÁLLÍTÁSA

A **rosszindulatú szoftverek és hackerek** a számítógépen futó szoftverek (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. A frissítések kiadásával az addig esetleg nem nyilvános hibákról is tudomást szerezhetnek a rosszindulatú szoftvereket készítők és a hackerek, így azok a rendszerek, amelyeken a hibákat javító frissítés nem történt meg fokozottan veszélyeztetettek lesznek.

Az operációs rendszer **automatikus frissítésének** bekapcsolásával biztosítható, hogy a számítógép a frissítés közzétételét követő legrövidebb időn belül megkapja a biztonsági frissítéseket. A felhasználói programok jelentős része szintén jelzi, hogy újabb verzió elérhető, ezek telepítése is ajánlott a fenti okok miatt.

BIZTONSÁGI TANÁCSOK

- Kapcsolja be az automatikus frissítéseket!
- Felhasználói fiókok felügyeletén állítsa be, hogy a kritikus műveletekhez (pl. program telepítése) a felhasználó engedélyére legyen szükség!
- Állítsa magasabb szintre a böngészők biztonsági beállításait!
- Ismeretlen eredetű szoftvereket ne telepítsen!
- Használjon vírusirtó programot!
- Kapcsolja be a tűzfalat a számítógépén vagy a routeren!
- Rendszeresen készítsen biztonsági mentést fontos adatairól!

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 vírusirtó 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 vírusirtó 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, 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 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.