Vírusok, spamek és a többiek...

AVAGY, MIRE FIGYELJÜNK EGY SZÁMÍTÓGÉPES HÁLÓZAT BIZTONSÁGÁVAL KAPCSOLATBAN

Sándor Zsolt

Napjainkban már szinte nincs olyan vállalkozás vagy család, ahol ne lenne legalább egy számítógép, természetesen internetes kapcsolattal. Ha pedig az internetre kapcsolódik, akkor esélyt ad a betolakodóknak, hogy kisebb vagy nagyobb kárt okozzanak számítógépes rendszerében.

Ilyen internetes betolakodók például a spamek (kéretlen reklámlevelek), a vírusok, a különböző spyware-ek, azaz kémprogramok, a hoax-ok és a joke-ok. A statisztikák szerint a vírusok 87%-a e-mailen érkezik, további 10% pedig az internetről történő adat letöltésekor kerül a rendszerbe.

Az ICSA felmérése alapján a szerverleállással járó incidensek 65%-ában egy óránál rövidebb volt az így elveszített idő, de mivel voltak olyan esetek is, ahol ezer óráig állnia kellett a szervereknek, az átlagos hozzá nem férési idő tizennégy órára jött ki. Ez egy vállalkozás esetében azt jelenti, hogy több mint egy egész munkanap volt az az idő, amely alatt bár a munkabérek és az egyéb költségek kifizetésre kerülnek, de a cég csak a kiesett bevételt realizálhatja! Ma már az ügyviteli rendszerek világában a szerverek kiesésével jellemzően megbénul a cégek működése. Ezenfelül még nem számoltunk a presztízsveszteséggel és az adatvesztés okozta károkkal!

Ugyanígy problémát jelentenek a beérkező spamek – nemkívánatos reklámüzenetek –, amelyek a beérkező levelek mintegy 67%(!)-a és a munkahelyen, a nem munkával kapcsolatos internetezéssel töltött idő, amely az informatikusok szerint heti 5,9 óra!

A spyware-ek, azaz a kémprogramok az egyik legjelentősebb internetes fenyegetettséggé váltak az utóbbi hónapokban. Az *IT Observer* szerint a számítógépek 90%-a fertőzött valamilyen típusú rosszindulatú kóddal. Ennek oka a malware-készítők olyan anyagi motivációja, mint például a nagymértékű profit, amely abból származik, hogy eladják a lehúzott adatokat vagy közvetlenül junkmaileket küldenek azokra.

A megfelelő biztonsági rendszer kiépítése minden felhasználó és hálózat számára egy megtérülő beruházás. Fontos, hogy a munkaállomás, illetve hálózat minden elemét, komponensét megfelelő védelemmel lássunk el.

A fentieket figyelembe véve, pedig válaszoljon néhány alapvető kérdésre!

- Védett-e számítógépe a tegnap megjelent új vírusok ellen?
- Rendelkezik-e automatikus vírusadatbázis-frissítéssel a szervereken vagy a munkaállomásokon?
- Védett-e a hálózata még ismeretlen fenyegetések ellen?
- Tudja-e ellenőriztetni az Ön számára fontos, de vírusgyanús fájlokat?
- Az Ön hálózatának minden belépési pontja védett?
- Kap-e értesítést a rendszergazda, ha valahol vírust észlel a vírusvédelmi rendszer?

Ha bármelyik kérdésre nemmel tud csak válaszolni, itt az ideje, hogy keressen egy komplex megoldást! Az ilyen problémákra kínál megoldásokat a **Panda Software,** amelynek védelmi rendszerei között a tűzfal, az antivírus, a preventív technológia, az anti-spyware, az anti-adware, az anti-spam és a webhozzáférés szűrés is megtalálhatók.