A tűz, avagy mi ellen véd a tűzfal? (kivonat)

Mátó Páter

2000. szeptember 27.

Egyre gyakrabban hallhatunk számítógépes rendszerek ellen elkövetett gonosztettekről. Ezeknek az akcióknak a célja leggyakrabban az erőfitogtatás, néha tiltakozás esetleg rosszindulat. Egy azonban biztos: ahogy egyre fontosabbak lesznek számítógépes rendszerek, úgy válnak egyre inkább egy-egy szervezet vagy ember Achilles-sarkává.
A rendszerek gyakran esnek áldozatául belső ember vagy szervezet akciójának. Ha a támadók az ellopni vagy megsemmisíteni szándékozott információkhoz legálisan hozzáférhetnek, akkor a támadás megakadályozása szinte lehetetlen. Ha a megtámadni szándékozotti rendszerhez a támadóknak hozzáférése van ugyan, de nem elég magas szintű, akkor beszélhetünk lokális (számítógépen vagy hálózaton belüli) támadásról. Tételezzük fel, hogy a számítógéphez jogosan hozzáférő felhasználók jóindulatúak. Ebben az esetben a támadók a rendszert a számítógépes hálózaton keresztül igyekeznek hatalmukba keríteni.
Hogyan lehetséges, hogy egy nagy energiával felállított rendszer támadható? Hogyan kerülhetnek a programokba olyan hibák, melyek a teljes rendszer kompromittálódásához vezethetnek? Mi a tűzfal és mi ellen véd? Mire kell figyelni egy szerver telepítésénél? Ezekre a kérdésekre kísérel meg választ adni ez az előadás.

A felvetett témákat a következő kérdéskörök tárgyalásán keresztül járja körül:

- A tipikus biztonságot veszélyeztető programozási hibák
  - Nyelvspecifikus programozási hibák
  - Nyelvfüggetlen programozási hibák
- A számítógépes hálózatokról
  - a hálózat felépítése
  - alacsony szintű támadások

  - a TCP/IP protokoll biztonsági kérdései

- A támadások fajtái és eszközei
  - félrevezetés (social engineering)
  - lehallgatás (sniffing)
  - címhamisítás (spoofing)
  - portscan
  - brute force
  - exploit-ok
  - DoS, DDoS
- A vég
  - várható maradványok
  - Újratelepítés
- Megelőzés
  - szolgáltatások szűrése
  - a naplók szerepe
  - csomagszűrő
  - folyamatos frissítés
  - wrapper-ek
  - alkalmazás tűzfalak