101

Spam és víruszûrési módszerek és tapasztalatok a PPKE ITK-n

Csillag Tamás
cstamas@itk.ppke.hu
Pázmány Péter Katolikus Egyetem, Információs Technológiai Kar

Napjaink égetõ problémái közé tartozik a spam és vírusszûrés. Nincs egyszerû megoldás, mivel mozgó célpontra kell tüzelni: a ,,gonosz'' technikái folyamatosan változnak, de az internet közösségben is sokan sokféle eszközzel segítik a rendszergazdák küzdelmét: programok, web helyek és szerver szolgáltatások állnak rendelkezésünkre, amik a levelek kezelését, szûrését, a fertõzött és rosszindulatú gépek kiiktatását teszik lehetõvé.

A PPKE ITK-n többféle kombinációban használunk ilyen eszközöket. A felhasznált eszközök mind szabad szoftverek. Ezért mód volt arra, hogy szükség szerint némelyik kódját is módosítsuk, továbbfejlesszük. Ezeket az eszközöket, összehangolásukat, továbbfejlesztéseiket és a közben szerzett tapasztalatokat foglalja össze az elõadás.

A spam és vírusszûrésben felhasznált eszközök: Postfix, Mailscanner, Exim, SpamAssasin, Clamav, Relaydb, Greylisting, Spam trap. Ezek közül valószínûleg a Relaydb és a greylisting az, ami kevésbé ismert. A relaydb-t OpenBSD-rõl kellett portolni, a greylisting kód a Wietse Venema munkájára épül. Mindkettõ igen hatékony eszköznek bizonyul.

A kialakított spam és vírusszûrési technológiát már több mint egy éve sikerrel alkalmazzuk az itk.ppke.hu, és a ppke.hu domainek mellett többek között a jak.ppke.hu, katolikus.hu, communio.hu, bioetika.hu domainek védelmére.