Dr. Illési Zsolt: Detektívkontroll-barát ITC rendszertervezés

A modern infokommunikációs (ICT) rendszerek biztonsági alrendszerének egyre komplexebb elvárásokat kell kielégítenie. Ezek közül az incidensek (váratlan rendszeresemények események, hibák, támadások stb.) előrejelzésért, korai felismeréséért és utólagos rekonstrukciójáért felelős funkciók jelenleg elsősorban a naplózásra és az IDS (Intrusion Detection System) megoldásokra fókuszálnak. A gyakorlatban azonban a detektív (felfedező) alrendszernek ezeknél összetettebb problémák megoldását is támogatnia kell:

- nem vagy csak részben szabályozott környezetben kell a szabályok megsértését észlelni,
- előre kell jeleznie a rendszer várható bizonytalanságait,
- fel kell fedeznie olyan szabálysértéseket, amelyek korában még nem fordultak elő,
- minimálisra kell csökkentenie az incidens és a felfedezése közti időt, hogy a szervezet reakcióidejét maximalizálja,
- az események rekonstrukcióját a szakemberek és a laikusok számára is értelmezhető formában kell megjelenítenie,
- megfelelő bizonyítékot kell szolgáltatnia egy esetleges munkajogi, polgári jogi vagy büntetőjogi eljáráshoz.

Az előadás összefoglalja azokat az általános jogi, üzleti és technikai követelményeket, amelyek alapján a zárt, teljes körű, folytonos felfedező biztonsági alrendszer funkciói megtervezhetőek, illetve példákat mutat a gyakorlati megvalósításukra.