2. DR. ZUTI PÁL:
AZ ADATVÉDELMI TUDATOSSÁG FEJLESZTÉSE. IT- ÉS INFORMÁCIÓBIZTONSÁG

A digitalizáció korában az információk feldolgozása, tárolása vagy szállítása általában az IT segítségével történik, de gyakran az információbiztonság még mindig analógabb, mint gondolnánk. Alapvetően az IT biztonság és az információbiztonság meglehetősen szorosan összefügg. Ezért a bizalmas információk, valamint magának az IT-nek a hatékony védelméhez szisztematikus megközelítésre, tudatosságfejlesztésre van szükség.

Az adatvédelem és az adatbiztonság nem szinonimái egymásnak! Adatvédelem alatt a személyes és érzékeny adatok jogszabályi védelmét érti a jogalkotó, adatbiztonság alatt pedig a számítógépes rendszerekben tárolt, feldolgozott, vagy továbbított adatok biztonságának fenntartására kell gondolnunk. A biztonság maga pedig egy a szervezet számára kedvező állapot, melynek megváltozása nem valószínű, de nem is kizárt.

Az információbiztonság három alapvető védelmi célja - bizalmasság, rendelkezésre állás és sértetlenség. Az információbiztonság tehát szélesebb körű, mint az IT-biztonság. Az IT-biztonság olyan állapot, amelyben az informatika használata során a fenyegetések és sebezhetőségek miatt fennálló kockázatokat megfelelő intézkedésekkel elfogadható szintre csökkentik. Az informatikai biztonság az az állapot, amelyben az információk és az informatika bizalmassága, sértetlensége és rendelkezésre állása megfelelő intézkedésekkel védett.

A felhasználók szempontjából jellemző, hogy az új készülékeket, webes szolgáltatásokat egyre többen veszik igénybe az életük egyre több területén. A népszerű készülékek (táblagépek, okostelefonok) könnyítik az életünket, ehhez azonban több különböző szolgáltatás – személyes információk – adatait szinkronizálják akár néhány perces gyakorisággal. Ennek a kényelemnek az a következménye, hogy a magán és a munkavégzéssel összefüggő adatok keverednek, és a biztonságuk is sérülhet. A világhálón elérhető szolgáltatások fejlődésével, a közösségi funkciók rendkívül dinamikus térnyerésével összefüggésben a biztonsági kockázatok számossága és a hatásuk mértéke is nő. Ma már természetes sokunknak olyan személyes adatok megadása akár nyilvános weboldalakon is, amelyet korábban csak közeli ismerőseinkkel, munkatársainkkal osztottunk meg. Egyes szolgáltatások világszintű népszerűségével, milliós felhasználói számukkal egy szoftver hiba, vírus vagy kártevő program károkozásának mértéke nagyságrendekkel nőhet.

A kulcsfontosságú informatikai területeken a nem kielégítő IT- és információbiztonság a legveszélyesebb. Ez jelenti a legnagyobb kockázatot. A digitalizáció hátulütője, hogy nő a digitalizált adatokkal való visszaéléseknek, a digitalizált adatok manipulálásának veszélye is! A rendszer megbízhatóság egy rendszer megbízható működésére vonatkozik, arra, hogy mennyire megbízhatóan áll a rendszer a felhasználók rendelkezésére, mennyire „üzembiztos”. A rendszerbiztonság alapvetően a rögzített adatok bizalmasságának és biztonságának a megőrzését jelenti. Az informatikai biztonság az informatikai rendszer olyan kedvező állapota, amelyben a kezelt adatok bizalmassága (confidentiality), sértetlensége (integrity) és rendelkezésre állása (availability) biztosított, valamint a rendszer elemeinek biztonsága szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos. Az alkalmazott technológiák meg kell, hogy védjenek a külső és belső támadásoktól, még a vezeték nélküli kommunikáció esetén is. Ezzel párhuzamosan biztosítani kell az adatok diszkrécióját és integritását. Az IT biztonság legkritikusabb kihívója maga a felhasználó! A felhasználók jelentik a legnagyobb „kihívást”, a felhasználók jelentik a legnagyobb IT-biztonsági kockázatot!