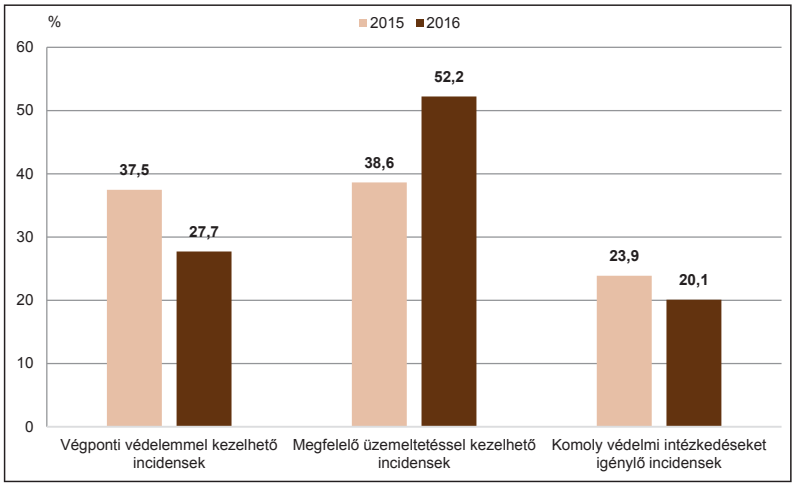
B.1.4. Kiberbiztonsági incidensek aránya a magyar közigazgatásban

A hálózatalapú információs rendszerek létfontosságú szerepet játszanak egy ország életében. Biztonságos működésük alapvető a gazdaság és a társadalom egésze szempontjából. Az információs rendszereket érő, azok működését veszélyeztető támadások nagyságrendje és gyakorisága folyamatosan növekszik, és ez a tendencia az előrejelzések szerint a jövőben csak erősödni fog.



Forrás: NKI

Egy ország kiberbiztonsági felkészültségének nemzetközileg egyik legelfogadottabb mutatója a közigazgatási szervezetek által jelentett információbiztonsági incidensek száma, ezen belül az egyes biztonsági események arányszáma. A bejelentett események típus szerinti eloszlása mutatja meg, hogy mennyire képesek a magyar közintézmények a komplexebb informatikai támadások felderítésére, valamint következtetni enged arra is, hogy milyen technológiai háttér és mekkora humán erőforrás áll rendelkezésre a magyar kibervédelemben. Minél többet költ egy kormányzat erre a területre, annál inkább képes lesz észlelni a nemzet biztonságát fenyegető, leggyakrabban rejtve maradó támadásokat. A biztonsági eseményeket a 2015-ben megalakult Nemzeti Kibervédelmi Intézetnek kell jelenteni. Az incidenstípusok az elhárítás szempontjából alapvetően három csoportra bonthatók.

Az első csoportba a legalapvetőbb védelmi technikákkal kezelhető incidensek tartoznak (a Nemzeti Kibervédelmi Intézet adatgyűjtésének kategóriái szerint ezek: a káros szoftver, a robothálózat és a kéretlen levél), ezeket a *Végponti védelemmel kezelhető incidensek* kategóriába soroljuk. Ezek 2016-ban az összes jelentett incidens 27,7%-át tették ki, az előző évhez képest 9,8%-os csökkenést mutatva. Ez köszönhető a kormányhivatalok elterjedésének és ezáltal a munkaállomások központi üzemeltetésének. A hatásos védelmi technikák beszerzése és üzemeltetése viszonylag egyszerű, így egyre több intézménynél használják őket.

A második csoportba azok az incidensek tartoznak, amelyek a rendszer-üzemeltetéshez, jellemzően az intézmény elektronikus szolgáltatásaihoz, szerverkörnyezetéhez kapcsolódnak. Ezt a kategóriát összefoglalva *Megfelelő üzemeltetéssel kezelhető incidensek*nek nevezzük (a Nemzeti Kibervédelmi Intézet adatgyűjtésének kategóriái szerint ezek: a sérülékeny szolgáltatások és a honlaprongálás). Az itt megmutatkozó incidensek hátterében jellemzően szakértő- és szakértelemhiány mutatkozik. A 2016-ban jelentett incidensek 52,2%-a tartozott ebbe a körbe, szemben az előző évi 38,6%-kal. A magyar közigazgatás erőteljes információtechnológiai centralizációja, valamint különböző központi szolgáltatások megjelenése segíthet ennek a problémának a megoldásában.

A harmadik csoportba tartoznak azok a támadások, amelyek általában nehezen észlelhetők, kezelésükhöz jelentős infrastruktúra-beruházás, illetve a felhasználók részéről komoly biztonságtudatossági fejlesztés szükséges, ezért ezeket *Komoly védelmi intézkedéseket igénylő incidensek* néven soroljuk be (a Nemzeti Kibervédelmi Intézet adatgyűjtésének kategóriái szerint ezek: az adathalászat, a túlterheléses támadás, a jogosulatlan hozzáférés, valamint a célzott támadás). A statisztikák szerint ezek okozzák a legkomolyabb károkat, sokszor mégis észrevétlenek maradnak. A 2016-ban jelentett incidensek 20,1%-a tartozott ebbe a körbe, ami enyhe csökkenést jelent a 2015-ben mért 23,9%-hoz képest.

A célzott támadások összesen 0,3%-ot tesznek ki az összes jelentett incidens között, valószínűsítve, hogy a nemzetbiztonságot potenciálisan fenyegető kibertámadások jórészt észrevétlenek maradnak.

A magyarországi kiberbiztonsági incidensek nagyobb része informatikai üzemeltetési hiányosságra vezethető vissza, a komplex támadások észlelési rátája nagyon alacsony.