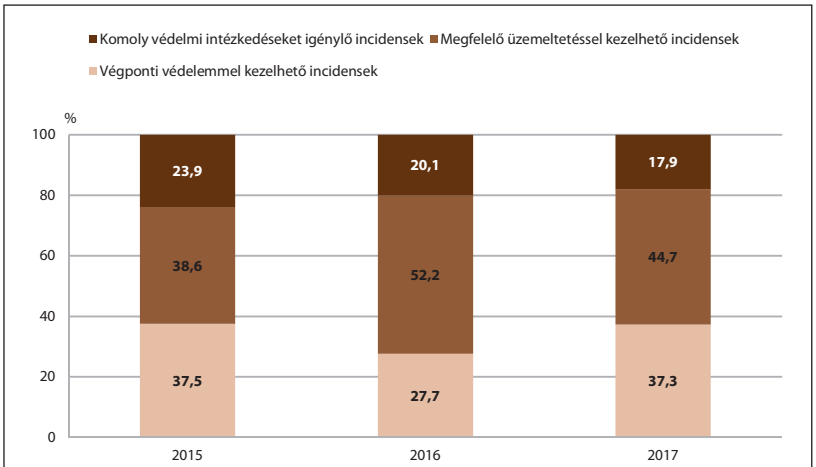
B.1.4. A magyar kiberbiztonság helyzete

A globalizációs folyamatok gyorsulásában a hálózatalapú információs rendszerek központi szerepet játszanak. Biztonságos működésük alapvető érdek a gazdaság fejlődése és a társadalom egésze szempontjából. Az információs rendszerek, a bennük előállított, tárolt, továbbított adatok, valamint a felhasználók által alkotott kibertér biztonsága érdekében szükséges, hogy Magyarország rendelkezzen azokkal a minimumképességekkel, amelyek biztosítani tudják a megfelelő szintű védelmet, és amelyek képessé teszik az országot a nemzetközi együttműködésekben való eredményes részvételre.



Kibervédelmi incidensek aránya a magyar közigazgatásban

Forrás: NKI

Magyarország esetében az információszabadságról szóló 2013. évi L. törvény kötelezővé teszi a biztonsági események jelentését. A bejelentett események típusainak eloszlása mutatja, hogy mennyire képesek a magyar közszolgálat szervezetei a komplexebb informatikai támadások felderítésére, egyben következtetni lehet arra, milyen technológiai háttér és mekkora humán erőforrás áll rendelkezésre a magyar kibervédelemben. Az incidenstípusok az elhárítás szempontjából három csoportra bonthatók.

Az első csoportba a legalapvetőbb védelmi technikákkal kezelhető incidensek tartoznak, ezeket a *végponti védelemmel kezelhető incidensek* kategóriába soroljuk. Ezek 2017-ben az összes jelentett incidens 37%-át tették ki, 9 százalékpontos növekedést mutatva az előző évhez képest.

A második csoportba azok az incidensek tartoznak, amelyek a rendszer-üzemeltetéshez, jellemzően az intézmény elektronikus szolgáltatásaihoz, szerverkörnyezetéhez kapcsolódnak. Ezeket *megfelelő üzemeltetéssel kezelhető incidensek*nek nevezzük, és jellemzően szakértő- és szakértelemhiányt tükröznek. 2017-ben a jelentett incidensek 45%-a tartozott ebbe a körbe, szemben az előző évi 52%-kal.

A harmadik csoportba tartoznak azok a támadások, amelyek általában nehezen észlelhetők, kezelésükhöz jelentős beruházás szükséges. Ezeket *komoly védelmi intézkedéseket igénylő incidensek*nek nevezzük. Az iparági statisztikák szerint ezek okozzák a legkomolyabb károkat, sokszor mégis észrevétlenek maradnak. 2017-ben a jelentett incidensek 18%-a tartozott ebbe a körbe, vagyis értéke érdemben nem változott a 2016-ban mért 20%-hoz képest.

A cél az, hogy a végponti védelemmel kezelhető incidensek és a megfelelő üzemeltetéssel kezelhető incidensek aránya a komoly védelmi intézkedéseket igénylő incidensek arányához képest csökkenjen. Ez azt jelentené, hogy Magyarország közigazgatásának kibervédelmi képességei érdemben javulnak, hiszen a rövid távon végrehajtható intézkedéseket megtette, az informatikai üzemeltetési hiányosságok kiküszöbölése egyre kevesebb incidenst eredményez, miközben kiépülnek azok az infrastruktúrák, amelyek a potenciálisan komoly hatású incidensek észlelését teszik lehetővé. Minél többet költ egy kormányzat a kibervédelemre, annál inkább képes észlelni a nemzet biztonságát fenyegető, de leggyakrabban rejtve maradó támadásokat.

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