



A HATÓSÁGI ELLENŐRZÉSEK TAPASZTALATAI

Selyem Zsuzsanna
NKI Hatósági Főosztály
zsuzsanna.selyem@nki.gov.hu

EGY KIS TÖRTÉNELEM...

2013. július 1. lbtv.
hatálybalépése

2014. július hatósági
ellenőrzések
megkezdése

2015. július 13.
hatóság az NBSZ

2020. július 1. alapvető
szolgáltatást nyújtó
szereplők



2014. július 1. az első
biztonsági osztályba és
-szintbe sorolások
határideje

2015. október 1.
NKI létrehozása

2019. január 1.
bejelentés-köteles
szolgáltatók

2020. július 31.
létfonosságú
rendszerelemek

A SZÁMOK BŰVÖLETÉBEN

Fő kötelezettségek:

- Szervezet és EIR felelős (IBF) regisztrációja 1202/1778
- IBSZ beküldése 1070/1778
- Biztonsági osztályba és –szintbe sorolás elvégzése 899/1778

ZÁRT, TELJES KÖRŰ, FOLYTONOS ÉS A KOCKÁZATOKKAL ARÁNYOS VÉDELEM

- *teljes körű védelem*: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem



- Tudjuk, hogy mit kell védeni – vagyonleltár: adatok(klasszifikáció), eszközök, szoftverek, kapcsolatok, erőforrások
- *kockázatokkal arányos védelem*: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével



- kockázatelemzés/-kezelés

ADMINISZTRATÍV INTÉZKEDÉSEK, AVAGY A MÁGIKUS GONDOLKODÁS DIADALA

- Idézetek: a BM rendelet kontrolljainak megisméltése egy szabályzatban nem jelenti egyben a megvalósítást is



- Nem minden kontrollhoz kell szükségszerűen adminisztratív szabályozónak tartoznia
- Folyamatok hiánya: nem fog teljesülni a feladat, ha nem írjuk hozzá a felelőst, a határidőt/gyakoriságot, és a végrehajtás konkrét módját



- Első a folyamat kialakítása, utána le is lehet írni

1000 FT ELÉG LESZ?! TÖBB NINCS!



- A biztonsági osztályba és –szintbe sorolást a kockázatok, és nem a lehetőségek oldaláról kell elvégezni
- A besorolásnál nem illik figyelembe venni a már meglévő védelmi intézkedéseket
- Elvárt és teljesített érték közötti különbség
- Felvállalt kockázatok – dokumentáltan!
- Helyettesítő intézkedések és egyéb eltérések

IBF – HELYE, SZEREPE

- **Ibtv. 13. § (1)** Az elektronikus információs rendszer biztonságáért felelős személy feladata ellátása során a szervezet vezetőjének közvetlenül adhat tájékoztatást, jelentést.



- kis „távolságra” a vezetéstől, függetlenség az üzemeltetéstől
- Együttműködés a menedzsmenttel, üzemeltetéssel, DPO-val
- „külsősöknek”: ne csak a dokumentumgyártás legyen feladat!



- folyamatok kiépítése, működés felügyelete

szabaduló
szoba

plakát
kampány

e-learning

TUDATOSÍTÁS!

csali e-mail

képernyős
tippek

hírlevelek

oktató
videók

KÖSZÖNÖM A FIGYELMET!