



HÍRKÖZLÉSI ÉS INFORMATIKAI
TUDOMÁNYOS EGYESÜLET
INFORMÁCIÓBIZTONSÁGI
SZAKOSZTÁLY

NEIH, - Ibtv. 14. § Osztályba sorolás és a
biztonsági szint ellenőrzési tapasztalatai,
biztonsági hiányosság elhárítása

Vereckei Béla

Biztonsági szint/biztonsági osztály 1.

- ▶ Szervezetek biztonsági szintje: a szervezet vagy szervezeti egység védelemre való felkészültségének szintje

Legalacsonyabb (1. szint) elvárásai: legyen egy olyan, a szervezetre érvényes, jogosult vezető által jóváhagyott, információbiztonsági felelősségeket, kötelezettségeket és felügyeleti képességet definiáló informatikai biztonsági szabályzata, amely ismert és betartott az érintett munkavállalók által, és amely tartalmaz kockázatelemzési eljárást, abba beépített ellenőrzési pontokkal.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 2013. július 1-én lépett hatályba, amelyben a szervezetek legalacsonyabb, 1. biztonsági szintjének elérésére (10. § (3) bek.) a jogalkotó a biztonsági szint felmérését követően 1 évet határozott meg. Ez a határidő 2015.01.01-től kettő , 2016. 06.18.-tól négy , majd 2017. 06.17.-től öt évre emelkedett. Ez azt jelenti, hogy a jelenleg hatályos szabályozás szerint azon jogalany szervezeteknek, amelyek az információbiztonsági tudatossági szintje a vizsgálat idején nem érte el a minimális szintet, azok számára 2019. 07.01.-ig nem is kötelező ezen szint elérése.

Biztonsági szint/biztonsági osztály 2.

- ▶ EIR biztonsági osztálya: az EIR, valamint az azokban kezelt adatok kockázatokkal arányosan biztosítható védelme érdekében, BSR kockázatok alapján 1-5-ig, a számozás emelkedésével párhuzamosan szigorodó, jogszabályban előírt védelmi előírások.
- ▶ Felügyelet: ellenőrzés (éves terv alapján)
 - ▶ tanácsadás; (igény szerint)
(hiányzó „szolgáltatás”: ajánlások)

Gyakorlati tapasztalataink/kihívások

- ▶ *Alacsony szintű incidens érzékelési képesség és bejelentési hajlandóság*
- ▶ *Elnyúló incidens reagálási idő, a kártékony kódok jelenlétének késői észlelése és azok kezelése minőségi- és időparaméter nélkül*
- ▶ *A szervezetek alacsony és lassan emelkedő IT biztonsági szintje*
- ▶ *A munkavállalók információbiztonsági tudatosságának hiánya/ alacsony szintje*
- ▶ *Azonosított legfőbb ok: „siló” jellegű projektgondolkodás (a végponti védelmi intézkedések (információbiztonsági elvárások a végponti hozzáférők részére) és anyagi fedezet biztosításának sorozatos elmulasztása*

Szakmai GYIK-elektronikus ügyintézés

- ▶ <http://neih.gov.hu/osztalyba-sorolas>
- ▶ <http://neih.gov.hu/szintbe-sorolas>
- ▶ http://neih.gov.hu/biztonsagi_osztaly_k%C3%B6vetelmenyei
- ▶ http://neih.gov.hu/biztonsagi_szint_kovetelmenyei

„Rokon” jogszabályok

▶ 2001. évi XXXV. törvény az elektronikus aláírásról

(A törvényt az Országgyűlés a 2001. május 29-i ülésnapján fogadta el. A kihirdetés napja: 2001. június 12. A törvényt a 2015: CCXXII. törvény 121. § (1) bekezdés a) pontja hatályon kívül helyezte 2016. július 1. napjával.)

▶ 2009. évi CLV. törvény a minősített adat védelméről

40. § (4) A nemzeti minősített adat védelmére vonatkozó fizikai és elektronikus biztonsági feltételeket 2020. december 31-ig kell megteremteni. (7. módosítás)