

VÁLTOZÁSOK AZ ELEKTRONIKUS INFORMÁCIÓBIZTONSÁG JOGI SZABÁLYOZÁSÁBAN

„A főbb sarokpontok 2019. január 1-ei
változások tükrében”

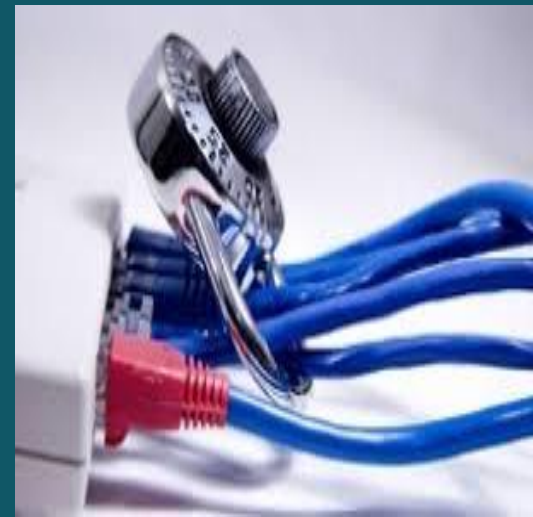
**Elektronikus
Információbiztonsági
Vezetők Okosan Klubja
Szakmai Fórum
2019. március 28.**

DR. BODÓ ATTILA PÁL

STRATÉGIAI SZINT

Az Európai Parlament és a Tanács 2016. július 6-i 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről

Forrás: <https://peworld.hu/kozelet/hacktivity-kozpontban-a-gyakorlati-kepzes-es-a-mobil-126485.html>



Magyarország hálózati és információs rendszerek biztonságára vonatkozó stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat – céljai alapjaiban azonosak a főáramlatokkal.

Célkitűzései: - digitális környezet iránti bizalom erősítése, digitális infrastruktúra védelem, gazdasági szereplők támogatása

- 1-56. pontja szerinti intézkedések végrehajtása érdekében intézkedési tervet kell készíteni 2019. 03. 31-ig.
- Alapvető szolgáltatók kijelölése vö. Lrtv. ágazati szereplők

FOGALMI ALAPVETÉSEK

EIR: a) elektronikus hírközlő hálózat - átviteli rendszerek a hálózatban jelek irányítására szolgáló berendezések, továbbá más erőforrások - beleértve a nem aktív hálózati elemeket is -, amelyek jelek továbbítását teszik lehetővé meghatározott végpontok között vezetéken, rádiós, optikai vagy egyéb elektromágneses úton, beleértve a műholdas hálózatokat, a helyhez kötött és a mobil földfelszíni hálózatokat, az energiaellátó kábelrendszereket, olyan mértékben, amennyiben azt a jelek továbbítására használják, a műsorszórásra használt hálózatokat és a kábeltelevíziós hálózatokat, tekintet nélkül a továbbított információ fajtájára;

b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy

c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok;

DE! - Maradt az Ibtv. 1. § (3) bekezdése [egy EIR-nek kell tekinteni adott adatgazda által, adott cél érdekében az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttesét].

+ új a honvédelmi célú elektronikus információs rendszer külön fogalma.

AZ IBTV. HATÁLYA

Központi államigazgatási szervek
(2019. 03. 01. Kit. és a
2010. évi XLIII. törvény)

Központi kormányzati igazgatási szervek:

- a) a Kormány,
 - b) a Miniszterelnöki Kormányiroda,
 - c) a minisztérium,
 - d) a kormányzati főhivatal, és
 - e) a központi hivatal.
- Kormányzati főhivatal (törvény által létrehozott, a Kormány irányítása alatt álló különös hatáskörű szerv vs. korábbi kormányhivatalok – KSH, OAH, SZTNH, NKFIH).
 - Központi hivatal: törvény vagy kormányrendelet által létrehozott, miniszter irányítása alatt álló különös hatáskörű központi szerv.



JOGKÖVETKEZMÉNYEK

1.	A jogszabálysértés megnevezése	A bírság legkisebb mértéke (Ft)	A bírság legnagyobb mértéke (Ft)
2.	regisztráció elmulasztása	50 000	100 000
3.	adattváltozás bejelentésének elmulasztása	50 000	500 000
4.	kockázatelemzés készítésének elmulasztása	200 000	500 000
5.	kockázatokkal arányos biztonsági intézkedések bevezetésének és alkalmazásának elmulasztása	300 000	5 000 000
6.	kockázatelemzés és a szükséges biztonsági intézkedések biztonsági eseményt követő haladéktalan, egyéb esetben évente dokumentált felülvizsgálatának elmulasztása, a felülvizsgálat során feltárt hiányosságok alapján a szükséges módosítások végrehajtásának elmulasztása	200 000	2 000 000
7.	biztonsági esemény bejelentésének elmulasztása	300 000	5 000 000
8.	hatóság végleges, végrehajtandó határozatában foglalt kötelezésének nem teljesítése	400 000	5 000 000

+ Az eljárás akadályozása, illetve az adatszolgáltatás nem vagy nem megfelelő teljesítése esetén 3 millió Ft-ig terjedő bírsággal sújthatja - **ismételt jogsértés esetén sújtani köteles - a jogsértő vezető tisztségviselőjét is.**

JOGKÖVETKEZMÉNYEK

- ✓ Kötelező hatósági felhívás: hiányosság, mulasztás, a biztonsági követelmény megsértése megszüntetésére, jogszabályban meghatározott kötelezettség teljesítésére, az elvárt intézkedés megtételére;
- ✓ Azonnali intézkedésekre kötelezés (súlyos biztonsági esemény) + fegyelmi felelősség megállapítására javaslat.
- ✓ Bírság szabható ki az eset összes körülményeinek mérlegelésével, amely további nem teljesülés esetén megismételhető.
- ✓ Költségvetési szerv esetén ha a felszólítás ellenére nem teljesít a hatóság felügyeleti szervhez fordulhat, ennek eredménytelen eltelte esetén kezdeményezheti az információbiztonsági felügyelő kirendelését + jogosult bírságot kiszabni.
- ✓ Mérlegelési jogkör megmaradt!
 - a) az elektronikus információbiztonságot veszélyeztető hiányosság, mulasztás, a megsértett biztonsági követelménynek a biztonsági osztályba sorolás és biztonsági szint szerinti súlyát,
 - b) történt-e súlyos biztonsági esemény, vagy fennállt-e ilyen esemény bekövetkeztének veszélye,
 - c) a biztonsági esemény hatását, vagy lehetséges hatását az érintett szervezetre, vagy más szervezetekre,
 - d) az érintett szervezet magatartását, hatósággal való együttműködését és
 - e) az esemény egyedi, vagy ismételt jellegét.

ÚJ VHR SZABÁLYOK

*az eseménykezelő központok feladat- és hatásköréről,
valamint a biztonsági események kezelésének és
műszaki vizsgálatának, továbbá a
sérülékenységvizsgálat lefolytatásának szabályairól
szóló 271/2018. (XII. 20.) Korm. rendelet*



Forrás:
<https://jogvadasz.com/2016/10/03/vegrehajtasi-eljaras/>

- ✓ NIS irányelv szerinti módosítás (alapvető szolgáltatók, CSIRT hálózat fogalmi szinten)
- ✓ Eseménykezelő Központ feladat- és hatáskörének újraszabályozása + Ibtv. módosítás
- ✓ Együttműködési kötelezettség átszervezése
- ✓ Biztonsági események bejelentése (alapvető szolgáltatóra vonatkozó speciális szabályok) vö. alaptartalom (rövid leírás, státusz, a szolgáltatás működésében támadt zavar mértéke, kezelésre kijelölt és közvetítő szolgáltató elérhetőségei, a hatást meghatározó szempontok).
- ✓ Önkéntes bejelentés (Lrtv. Ágazatok, akik nem alapvető szolgáltatók) vö. olyan kötelezettség nem írható elő, ami a bejelentés megtétele nélkül ne vonatkozott volna a bejelentőre)

ÚJ VHR SZABÁLYOK

271/2018. (XII. 20.) Korm. rendelet vö. biztonsági esemény kivizsgálása Együttműködési kötelezettség kiterjesztése a biztonsági esemény kivizsgálása során (bejelentő vs. Központ)

- *információátadás* (érintettek beazonosításához szükséges műszaki, technikai adatok, a biztonsági események kezeléséhez szükséges műszaki, technikai adatokat, információk kérésre történő átadása vagy hozzáférhetővé tétele, adott esetben ezeket a Központ begyűjtheti)
 - *tájékoztatás* (megtett intézkedésekről, az infrastruktúrával kapcsolatos beállításokról, alapvető szolgáltatást nyújtók esetén, speciális, ágazati sajátosságokról)
 - *hozzáférés* (az incidensben érintett infrastruktúrához, a Központ által végzett kockázatelemzés alapján szükségesnek ítélt korai figyelmeztető- vagy csapdarendszerek, szenzorok telepítésére)
 - *helyszíni tanácsadás*: központ képviselője helyszíni tanácsadás keretein belül, az érintett szervezet szakértőinek bevonásával javaslatot tesz a szükséges adatok összegyűjtésének és biztosításának módjára
- + alapvető szolgáltatást nyújtók a Központ kérésére kötelesek szükség szerint tiltásokat bevezetni, illetve (felhasználói, előfizetői) hozzáféréseket korlátozni, felfüggeszteni vagy megszüntetni.
- + Központ a biztonsági eseménnyel érintett szervezettel együttműködve dolgozza ki a biztonsági esemény felszámolásához szükséges intézkedéseket, melyeket a biztonsági eseménnyel érintett szervezet köteles végrehajtani.

ÚJ VHR SZABÁLYOK

az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet
12/A. Az EIR-ek biztonságáért felelős egyedüli kapcsolattartó pont

Hatóság, mint kijelölt szervezet, amely főbb feladatai:

- a) hatóságok és az érintett EGT tagállamok hatóságai közötti együttműködés,
- b) együttműködés az eseménykezelő központtal,
- c) alapvető szolgáltatók EIR-jei esetében a megfelelés vizsgálatával összefüggő adatok és a vizsgálat eredményének megküldése az Európai Bizottság részére, az érintett adatok:
 - az alapvető szolgáltatók azonosítását lehetővé tevő nemzeti intézkedések,
 - az alapvető szolgáltatások jegyzéke,
 - az alapvető szolgáltatók száma, valamint az érintett ágazat szempontja szerinti jelentőségük,
 - az adott szolgáltatásra támaszkodó felhasználók száma, vagy az alapvető szolgáltatásokat nyújtó gazdasági szereplő ellátási szintje, valamint
 - az eseménykezelő központok hatásköréről, és a biztonsági események kezelésére szolgáló eljárásról szóló tájékoztatás.
- d) az alapvető szolgáltatók és a bejelentés-köteles szolgáltatók EIR-jeiben bekövetkezett biztonsági eseményről az érintett tagállamok tájékoztatása, ha a biztonsági esemény jelentős zavart okozott a szolgáltatás nyújtásában,
- e) Együttműködés a magyar és a nemzetközi hálózatbiztonsági szervekkel, különösen az Együttműködési csoporttal és a CSIRT-ek hálózatával,
- f) szükség szerinti konzultációt folytatása és együttműködés a rendvédelmi szervekkel, illetve a NAIH-al.

ÚJ VHR SZABÁLYOK

az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről szóló 270/2018. (XII. 20.) Korm. rendelet

- Hatály: Ekertv. szerinti bejelentés köteles szolgáltató és közvetítő szolgáltató, kivéve ha létfontosságú rendszerelem
- Szervezetek - a bejelentés-köteles szolgáltatást nyújtók esetében: ellenőrzés hatóság, biztonsági események bejelentése eseménykezelő központ
- Hatósági jogkörök: nyilvántartás, kapcsolattartás, adatszolgáltatásra kötelezés,
- Jelentős biztonsági események bejelentése az alábbi adattartalommal:
 - a) a biztonsági esemény által érintett felhasználók számát, különös tekintettel azon felhasználókra, akik az érintett szolgáltatásra alapozzák a saját szolgáltatásaik nyújtását,
 - b) a biztonsági esemény időtartamát,
 - c) a biztonsági esemény által érintett terület földrajzi kiterjedését,
 - d) a szolgáltatás működésében támadt zavar mértékét,
 - e) a gazdasági és társadalmi tevékenységekre gyakorolt hatás mértékét.
- Jogkövetkezmények:
- Felhívás hiányosság, mulasztás megszüntetésére, kötelezettség teljesítésére, elvárt intézkedés megtételére
- Súlyos biztonsági esemény fenyegetése esetén azonnali intézkedésre kötelezés + javaslattétel fegyelmi felelősségre
- Bírság kiszabása, regisztráció, biztonsági esemény bejelentésének, alapvető követelmények teljesítésének, hatósági döntések foglaltak teljesítésének elmulasztása.

ÚJ VHR SZABÁLYOK

270/2018. (XII. 20.) Korm. Rendelet

- + Több szabálytalanság együttes fennállása esetén az egyes szabálytalanságokért kiszabható bírságok összege nem haladhatja meg az 5 Ft-os felső határt.
- + A bírság megfizetése nem mentesít a büntetőjogi, a polgári jogi felelősség, valamint a bírság kiszabására okot adó szabálytalanság megszüntetésének kötelezettsége alól.
- + A bírság ugyanazon tényállás mellett - az azonnal megszüntethető szabálytalanságok kivételével - a bírságot kiszabó végleges határozat közlését követő két hónap elteltével szabható ki ismételten.

1.	A jogszabálysértés megnevezése	A bírság legkisebb mértéke (Ft)	A bírság legnagyobb mértéke (Ft)
2.	regisztráció elmulasztása	50 000	100 000
3.	adatváltozás bejelentésének elmulasztása	50 000	500 000
4.	kockázatelemzés készítésének elmulasztása	200 000	500 000
5.	kockázatokkal arányos biztonsági intézkedések bevezetésének és alkalmazásának elmulasztása	300 000	5 000 000
6.	kockázatelemzés és a szükséges biztonsági intézkedések biztonsági eseményt követő haladéktalan, egyéb esetben évente dokumentált felülvizsgálatának elmulasztása, a felülvizsgálat során feltárt hiányosságok alapján a szükséges módosítások végrehajtásának elmulasztása	200 000	2 000 000
7.	biztonsági esemény bejelentésének elmulasztása	300 000	5 000 000
8.	hatóság végleges, végrehajtandó határozatában foglalt kötelezésének nem teljesítése	400 000	5 000 000

AMI MÉG VÁRHATÓ

- ✓ T/5237. számú törvényjavaslat az egyes ügyintézési folyamatok egyszerűsítéséről – Ibtv. 9. § módosítása – a hatóság előzetes engedélyének törlése ha a létfontosságú rendszerelem esetén a szervezet biztonsági szintjének alacsonyabb szintű meghatározására kerül sor.
- ✓ Magyarország hálózati és információs rendszerek biztonságára vonatkozó stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat szerinti intézkedési terv 2019-2022 közötti időszakra (potenciális területek: biztonság tudatosság, kibervédekezés, elhárítási és reagálási képesség, bűnüldözés, intézményrendszer)
- ✓ Szervezetkonszolidáció ?
- ✓ Együttműködés, személyi és szervezeti tudatosítás a részes felek oldaláról .

KÖSZÖNÖM A FIGYELMET!