

# A kormányzati IT biztonság aktualitásai

Kormányzati Eseménykezelő Központ (GovCERT-Hungary)  
Nemzeti Kibervédelmi Intézet

Dr. Bencsik Balázs

# Egy kis történelem

- 2013. július 1.: hatályba lép az Ibtv.
- Heterogén szervezetrendszer:
  - Hatósági feladatok: NEIH (NFM) + a kivételek (BM, NGM, HM, ME, KÜM)
  - Szakhatóság (sérülékenységvizsgálat): NBF (KIM)
  - Kormányzati CERT: NBSZ (BM)
  - Kiberbiztonsági Koordináció (Miniszterelnökség)
- Nehézkes együttműködés, szakemberhiány, forráshiány, infóhiány...
- 2014: e-közigazgatás és IT biztonság felelőse a BM
- 2015: Ibtv felülvizsgálat, további feladatkoncentráció

# Új szervezeti modell (2015- )



# CERT tevékenység (2013- )

A CERT fő küldetése:

- azonnali segítség a bajban (incidenskezelés)
  - 7/24 ügyeleti szolgálat
  - koordinációs és technikai támogatás
- szakértő támogatás a megelőzésben (sérülékenységek, fenyegetések)
  - kutatás, tájékoztatás, riasztás
  - tudatosítás, gyakorlatok
- kapcsolat a nemzetközi vérkeringésbe (FIRST, TI, IWWN, CECSP)
  - információcsere, együttműködés

# Nemzetközi és hazai együttműködés

Együttműködés az ügyfelekkel: szolgáltatásnyújtás

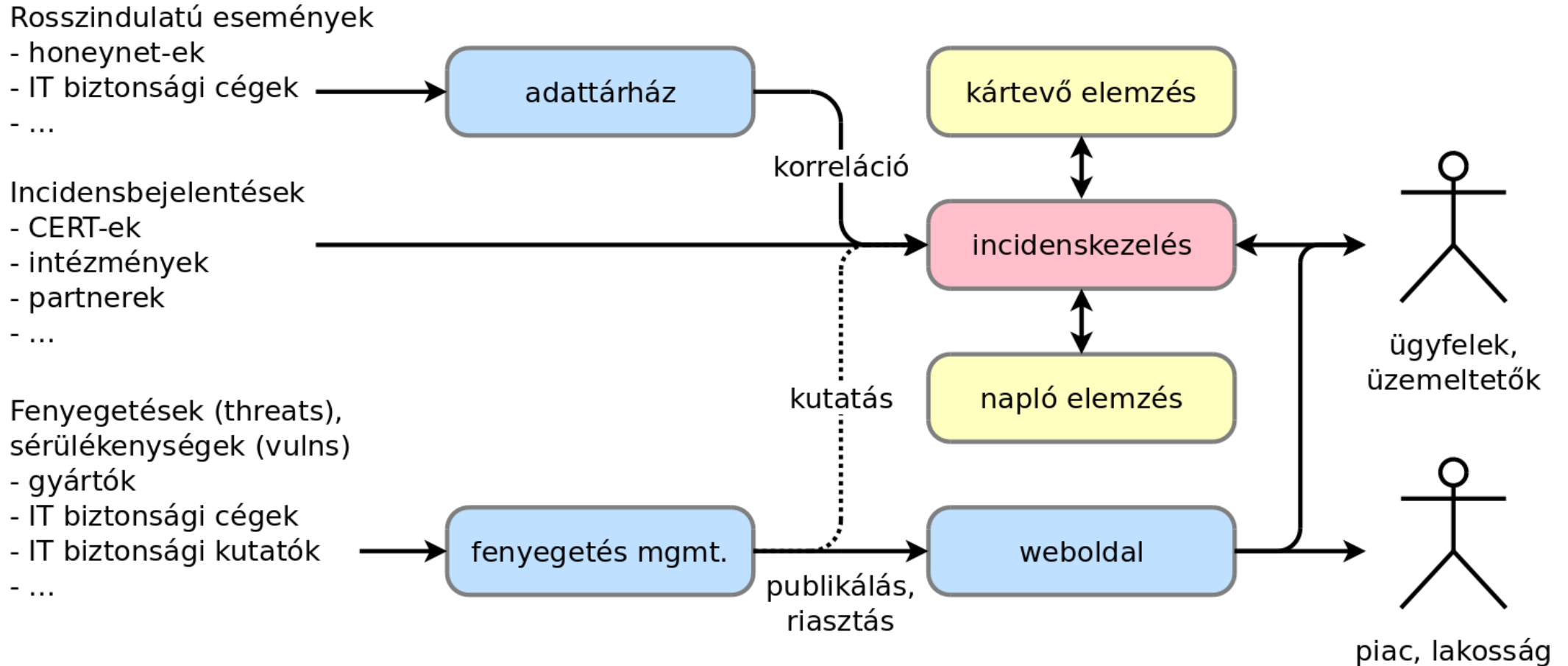
Együttműködés a rendvédelmi szervekkel

Együttműködés az iparági szereplőkkel

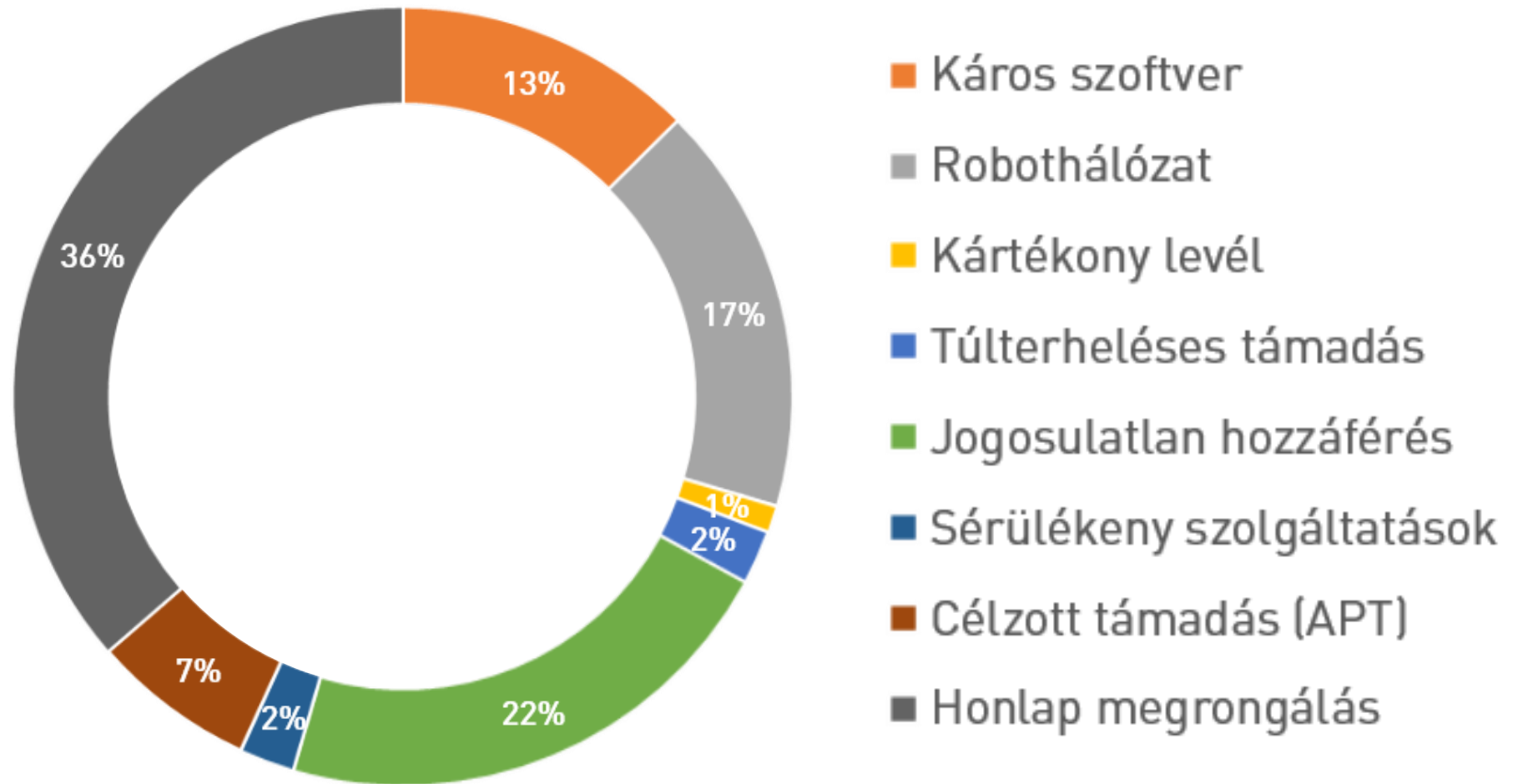
- szolgáltatók (ISP/content/hosting/...): incidenskezelés, hardening
- IT-biztonsági cégek, akadémia: információcsere, oktatás
- szoftverfejlesztők: biztonsági hibajavítások (coordinated disclosure)

Együttműködés a nemzetközi CERT közösségekkel: folyamatos információcsere, jó gyakorlatok átvétele, inspiráció

# CERT folyamatok, szolgáltatások



# Incidensek (2015Q2)



# Mi nem a GovCERT?

- nem SOC
- nem avatkozunk be ügyfeleink rendszerébe
- nem alkalmazunk “aktív védelmet”, sem „ellencsapást”
- nem rendőrség



# Nemzeti Elektronikus Információbiztonsági Hatóság

- Létrehozta az lbtv. 2013. július 01. NFM
- 2015. január 01. e-közigazgatásért felelős miniszter (BM)
- 2015. július 16. lbtv. módosítás, NBSZ

NBSZ 301. Főosztály, 3013. Hatósági Osztály

# Hatósági jogalkalmazási eljárások

- Nyilvántartások
  - nyilvántartások vezetése
- Engedélyezések/hozzájárulások
  - EGT tagállamaiban történő elektronikus információs rendszer üzemeltetése tekintetében engedélyezési eljárás lefolytatása
- Kötelezések
  - a feltárt hiányosságok pótlásának elrendelése, ellenőrzése
- Szankcionálások
  - felszólítás, bírság
  - felszólítás után információbiztonsági felügyelő kirendelésének kezdeményezése

# Felügyeleti eljárás

- Helyszíni ellenőrzés éves ellenőrzési terv alapján (fizikai, logikai)
- Beküldött iratok alapján történő hivatali ellenőrzés (adminisztratív),
  - osztályba és biztonsági szintbe sorolás,
  - IBSZ,
  - IBF,
  - cselekvési terv ,
- A fejlesztési projektek tervezési szakaszában ellenőrizni az információbiztonsági követelmények megtartását
- Kockázatelemzés

# Hatóság egyéb feladatai

- Javaslattevés a nemzeti létfontosságú rendszerrelem kijelölésére, együttműködés az ágazati kijelölő hatóságokkal
- Együttműködés az Elektronikus Ügyintézési Felügyelettel
- Kapcsolattartás (NB szolgálatok, eseménykezelő központok)
- Honlapon közzététel – riasztások (GovCERT)
- Hazai gyakorlatok szervezése, nemzetköz gyakorlatokon képviselheti Magyarországot

# Sérülékenységvizsgálat

A tevékenység újraszabályozása:

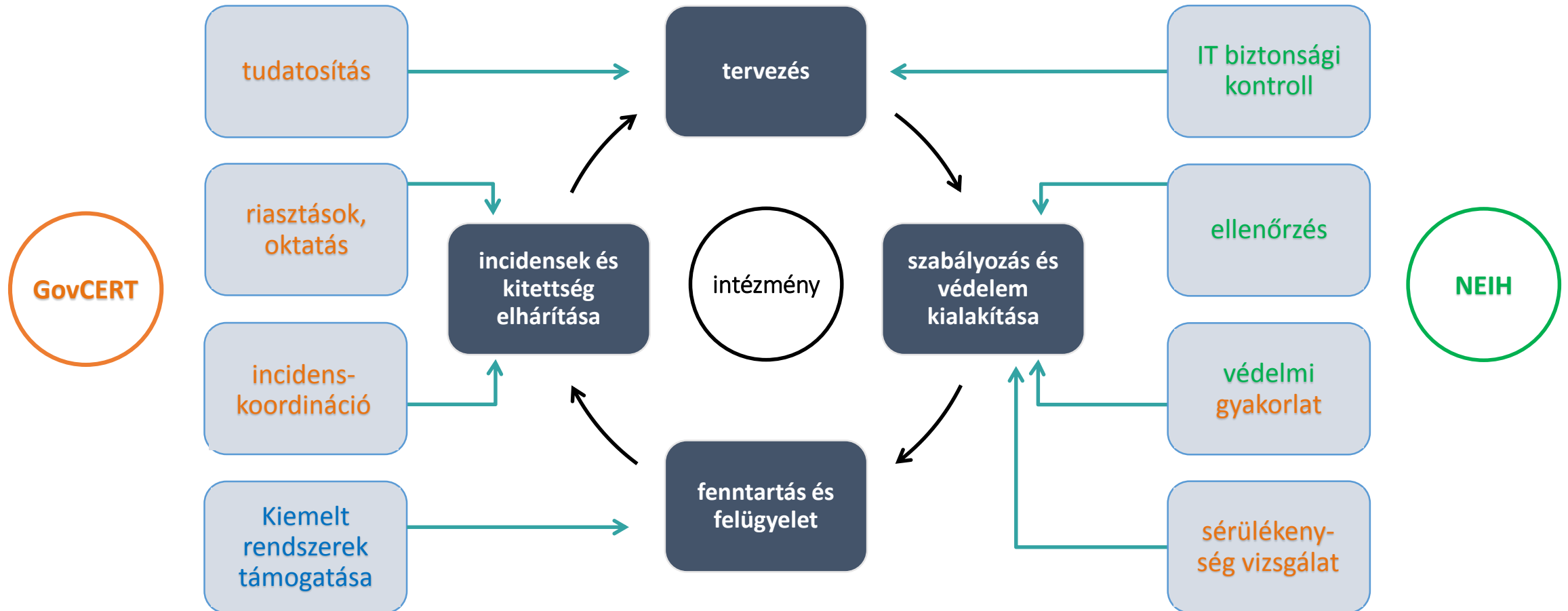
- Nem (szak)hatósági aktus!
- Minden esetben az érintett szerv rendeli meg a vizsgálatot:
  - Önként (pl. új e-közzolgáltatás bevezetése), vagy hatósági kötelezésre
- Meghatározott szervektől rendelheti meg:
  - GovCERT: NB védelem alá tartozó szerv (Ibtv!), létfontosságú rendszerek (Ibtv!), zárt célú rendszerek
  - Gazdasági társaság: egyéb állami és önkormányzati rendszerek
- Gazdasági társaság: TBT, NB ell., képesítés és 2 év gyakorlat, AH lista

# Új feladatok, új kihívások

Komplex feladatrendszer egy szervezeten belül:

- GovCERT
- Hatósági feladatok
- Sérülékenységvizsgálat
- Kiemelt rendszereknél további biztonsági szolgáltatások
- Erőteljes tudatosítási tevékenység
- All-around megközelítés

# Kormányzati IT biztonsági életciklus



# Nemzeti Kibervédelmi Intézet

	GovCERT	NEIH
<b>Mit?</b>	technikai támogatás és vizsgálat	compliance támogatás és ellenőrzés
<b>Mikor?</b>	incidens esetén vagy igény szerint	a tervezőasztaltól folyamatosan
<b>Hogyan?</b>	incidenskoordináció, tájékoztatás, tudatosítás, oktatás, sérülékenységvizsgálat, gyakorlatok, ...	megfelelőségvizsgálat, állásfoglalások, ajánlások, fejlesztések IT biztonsági kontrollja, ...



## Aktuális állásajánlataink:

Pozíció	Kulcsszavak
Információbiztonsági szakértő	biztonságirányítás, kockázatelemzés, audit, tudatosítás
Informatikai biztonsági rendszermérnök	fejlesztés biztonsági kontrollja, biztonsági infrastruktúra támogatás
Fenyegetettség elemző	információelemzés, kutatás, információmegosztás, nemzetközi együttműködés
Informatikai biztonsági szakértő	sérülékenységvizsgálat
Rendszerfelügyeleti munkatárs	rendszerfelügyelet, naplóelemzés, incidenskezelés

Jelentkezés önéletrajzzal a [hr@govcert.hu](mailto:hr@govcert.hu) e-mail címen.

Kérdések?

Köszönöm a figyelmet!