
# Az incidenskezelés új korszaka

**Marsi Tamás**
NBSZ NKI
*tamas.marsi@nki.gov.hu*

# NIS – az eredeti ?!

- **Célja:** A NIS1 irányelv célja a hálózati és információs rendszerek biztonságának növelése az EU-ban
- **Kiberincidensek jelentési kötelezettsége**
- **Nemzeti hatóságok és együttműködés**
- **EU-szintű együttműködés**

# NIS2 – az új!

- Célja: Az EU kiberbiztonsági szintjének emelése
- Kiterjesztés a kritikus szektorokra
- Szigorúbb követelmények

# Kilövés előtt

- 2024. október 15-től 23-ig lezajlott a Magyarország kiberbiztonságáról szóló törvénytervezet társadalmi egyeztetése, október 29-ig pedig  benyújtásra került az Országgyűlés elé.

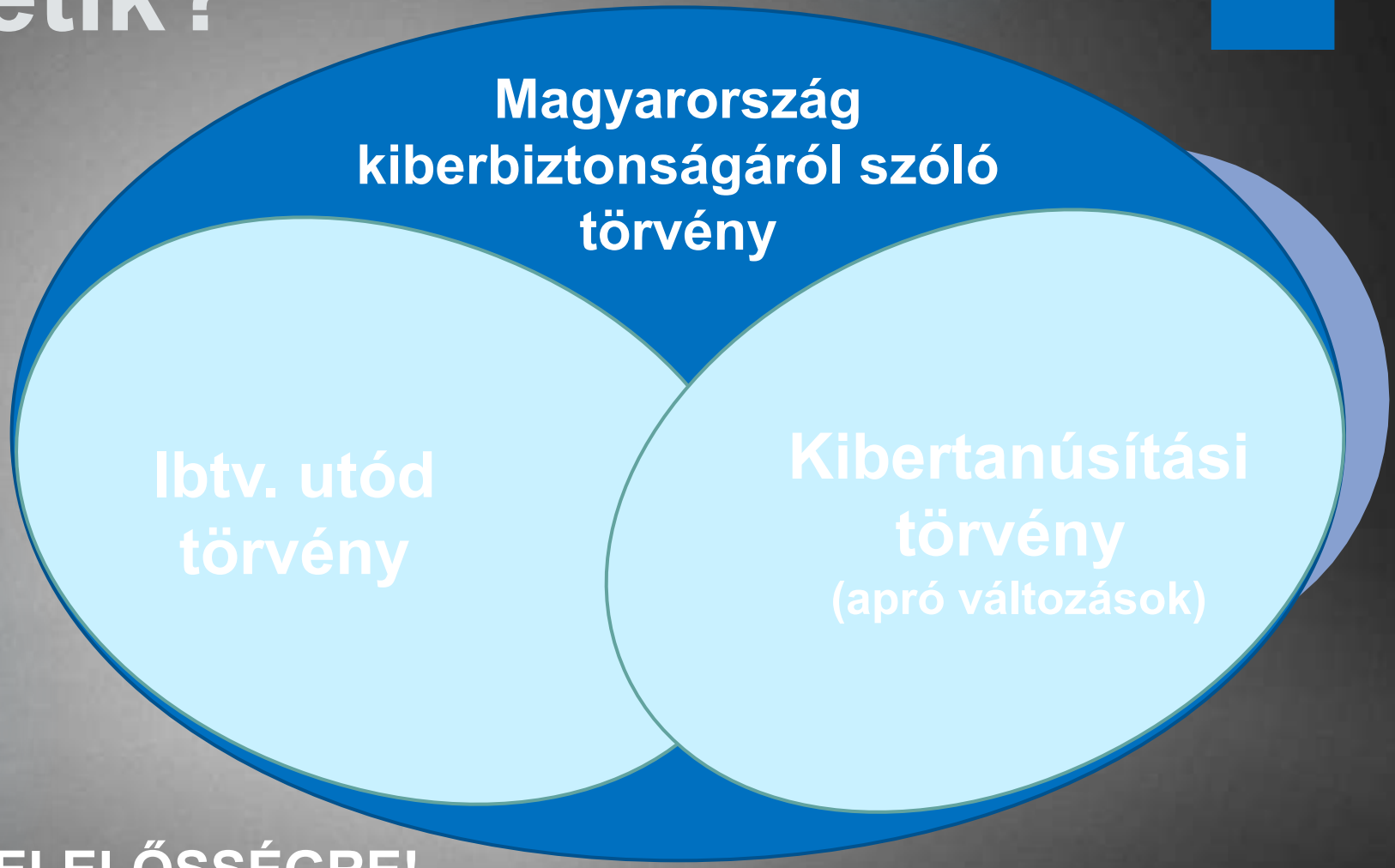
- *https://kormany.hu/dokumentumt ibe*

# Tervezett további lépések


- 2024. november-december – parlamenti jóváhagyás
- 2025. január 1. – hatályba lépés
- Végrehajtási kormányrendelet kiadása

- Finishez közelít még: a kritikus szervezetek ellenálló képességéről szóló törvény (Lrtv. utóda, CER implementáció)

# Mi születik?




**CSAK SAJÁT FELELŐSSÉGRE!**

**Az alábbiak a mai napon még tervezetként kezelendők!**

# KIBERBIZTONSÁGI HATÓSÁGOK / INCIDENSBEJELENTÉS

## KIBERBIZTONSÁGI HATÓSÁGOK/ESEMÉNYKEZELŐK

ÁLLAMI SZEREPLŐK
(kivéve honvédelem)

SZTFH

NEMZETI KIBERVÉDELMI INTÉZET

MAGYAR NEMZETI BANK

KIBERTAN TV. ALANYOK

NIS2 ÁGAZGATOK

PÉNZÜGYI SZEREPLŐK

HONVÉDELMI ÁGAZAT

# NKI KORLÁTAI

**AZ NBSZ NKI-NAK NINCS NYOMOZATI JOGKÖRE**

**NINCS FOGYASZÓVÉDELMI HATÓSÁGI JOGKÖR**

**ADATVÉDELMI HATÓSÁGI JOGKÖR HIÁNYA**

**POLGÁRI JOGI VITÁKBAN NINCS JOGKÖRÜNK ELJÁRNI**

# FOGALMAK

Kiberbiztonsági incidens

**Confidentiality – Bizalmasság:** Az információk védelme, valamint annak a biztosítása, hogy csak jogosult személyek férhessenek hozzá a fájlokhoz és a fiókokhoz.

**Integrity – Sértetlenség:** A tárolt adatok valóban megfelelnek a tárolni kívánt információknak, megfelelő felhatalmazás nélkül senki ne szúrjon be, módosítson vagy töröljön semmit.

**Availability – Elérhetőség:** Szükség szerint hozzá lehessen férni a rendszerekhez és az adatokhoz.

Üzemeltetési kiberbiztonsági incidens rendelkezésre állását nem szándékoltan csökkenti vagy megszünteti

Karbantartások!

Nemzeti kiberbiztonsági incidenskezelő központ:

- CSIRT
- CERT

Ágazaton belüli kiberbiztonsági incidenskezelő központ:

# FOGALMAK

## Jelentős kiberbiztonsági incidens

- a szolgáltatás **legalább 5%-os csökkenésével** vagy a szervezet **éves bevételének legalább 5 %-os kiesésével** jár vagy fenyeget;
- **súlyos működési zavart** okoz vagy képes okozni a szolgáltatásokban, vagy **pénzügyi vagy reputációs veszteséget okoz** vagy képes okozni
- jelentős vagyoni vagy nem vagyoni kár okozásával más **természetes vagy jogi személyeket érintett**, vagy képes érinteni
- üzleti titkok kiszivárgását okozta vagy okozhatja

## Nagyszabású kiberbiztonsági incidens

- mértékű zavart okoz
- **meghaladja Magyarországnak az arra való reagálási képességét**
- amely Magyarországra és legalább még egy másik országra jelentős hatást gyakorol

# INCIDENSEK BEJELENTÉSE

**24 ÓRA**

**72 ÓRA**

**EGY HÓNAP**

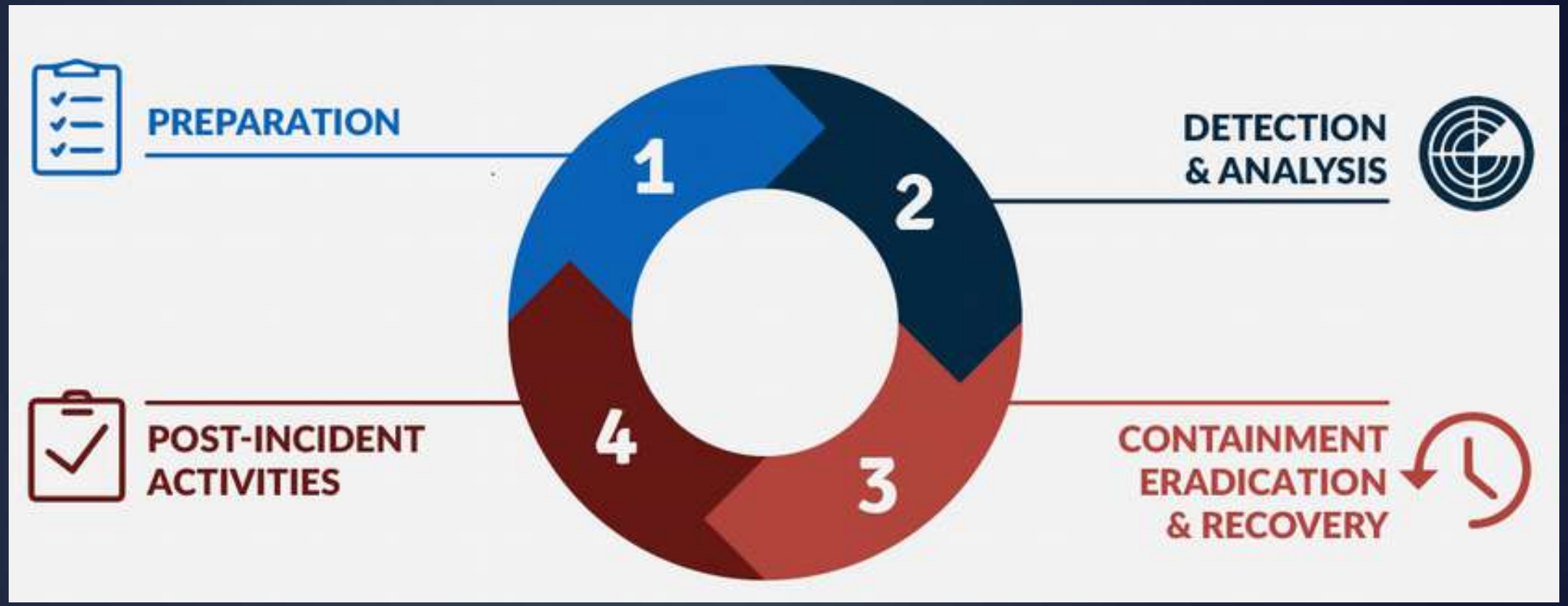
# Jogkövetkezmények

| | A | B | C |
|---|---|---|---|
| | A jogszabálysértés megnevezése | A bírság legkisebb mértéke (forint) | A bírság legnagyobb mértéke (forint) |
| 1. | az elektronikus információs rendszer biztonságáért felelős személy hatósági nyilvántartásba vételére irányuló kérelem benyújtásának elmulasztása | 200.000 | 2.000.000 |
| 2. | információbiztonsági szabályzat hatósági nyilvántartásba vételére irányuló kérelem benyújtásának elmulasztása | 200.000 | 2.000.000 |
| 3. | biztonsági osztályba sorolási kötelezettség elmulasztása | 200.000 | 4.000.000 |
| 4. | az elektronikus információs rendszer biztonságáért felelős személy adatainak módosítására irányuló kérelem benyújtásának elmulasztása | 200.000 | 2.000.000 |
| 5. | alapvető kiberhigiéniai gyakorlatok és kiberbiztonsági képzések szervezése vagy az ezeken való részvétel igazolásának elmulasztása | 400.000 | 4.000.000 |
| 6. | eseménykezelő központtal való együttműködési kötelezettség elmulasztása | 500.000 | 50.000.000 |
| 7. | a kiberbiztonsági hatóság vagy az eseménykezelő központ által elrendelt sérülékenységvizsgálati, illetve esemény kivizsgálási kötelezettség elmulasztása | 500.000 | 50.000.000 |

# Jogkövetkezmények

| | | | |
|---|---|---|---|
| 8. | a kiberbiztonsági hatóság által jóváhagyott sérülékenységkezelési terv szervezet általi végrehajtásának elmulasztása | 200.000 | 10.000.000 |
| 9. | arányos biztonsági intézkedések bevezetésének és alkalmazásának elmulasztása | 200.000 | 10.000.000 |
| 10. | a kiberbiztonsági incidens bejelentésének elmulasztása | 500.000 | 5.000.000 |
| 11. | a szervezet által nyújtott szolgáltatás igénybe vevői, illetve az egyéb érintettek részére elrendelt tájékoztatási kötelezettség elmulasztása | 2.000.000 | 20.000.000 |
| 12. | zárójelentés elkészítésnek elmulasztása, illetve nem megfelelő módon történő teljesítése | 500.000 | 5.000.000 |
| 13. | a kiberbiztonsági hatóság végleges, végrehajtható határozatában foglalt kötelezésének nem teljesítése | 1.000.000 | 50.000.000 |
| 14. | az információbiztonsági felügyelővel való együttműködés elmulasztása | 1.000.000 | 40.000.000 |
| 15. | közvetítő szolgáltató együttműködési kötelezettségének megszegése | 1.000.000 | 40.000.000 |

# Incidenskezelés folyamata



# Védekezés

- Megelőzés
- Megerősítés
- Monitorozás
- Tudatosítás

# Védekezés – csak mint a leggyengébb pont

# Eseménykezelés újdonságok

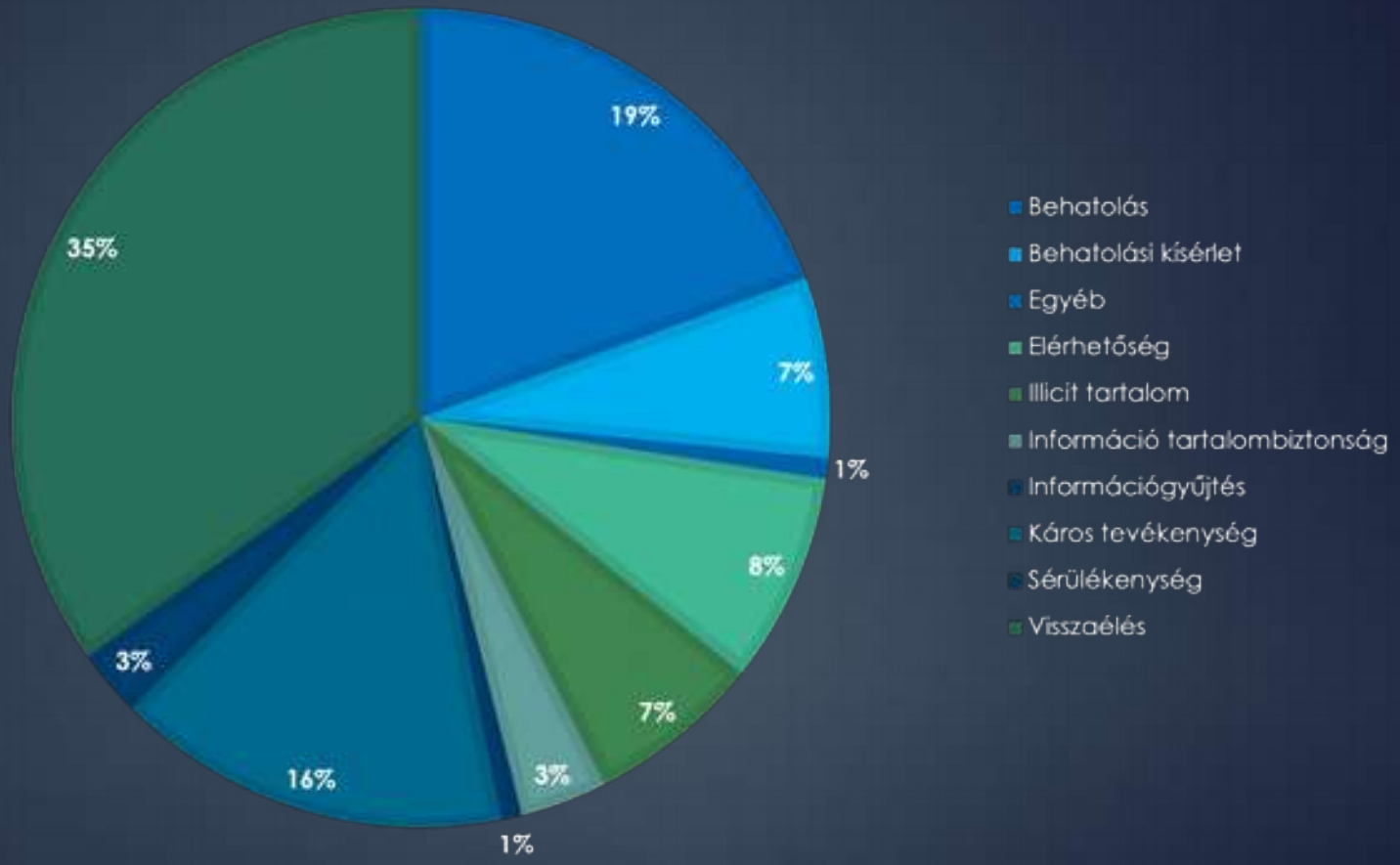
- önkéntes bejelentők
- kiberválságkezelés (EU-CyCLONe)
- kötelező gyakorlatok

CyCLONe
European Cyber Crises Liaison Organisation Network
Powered by ENISA

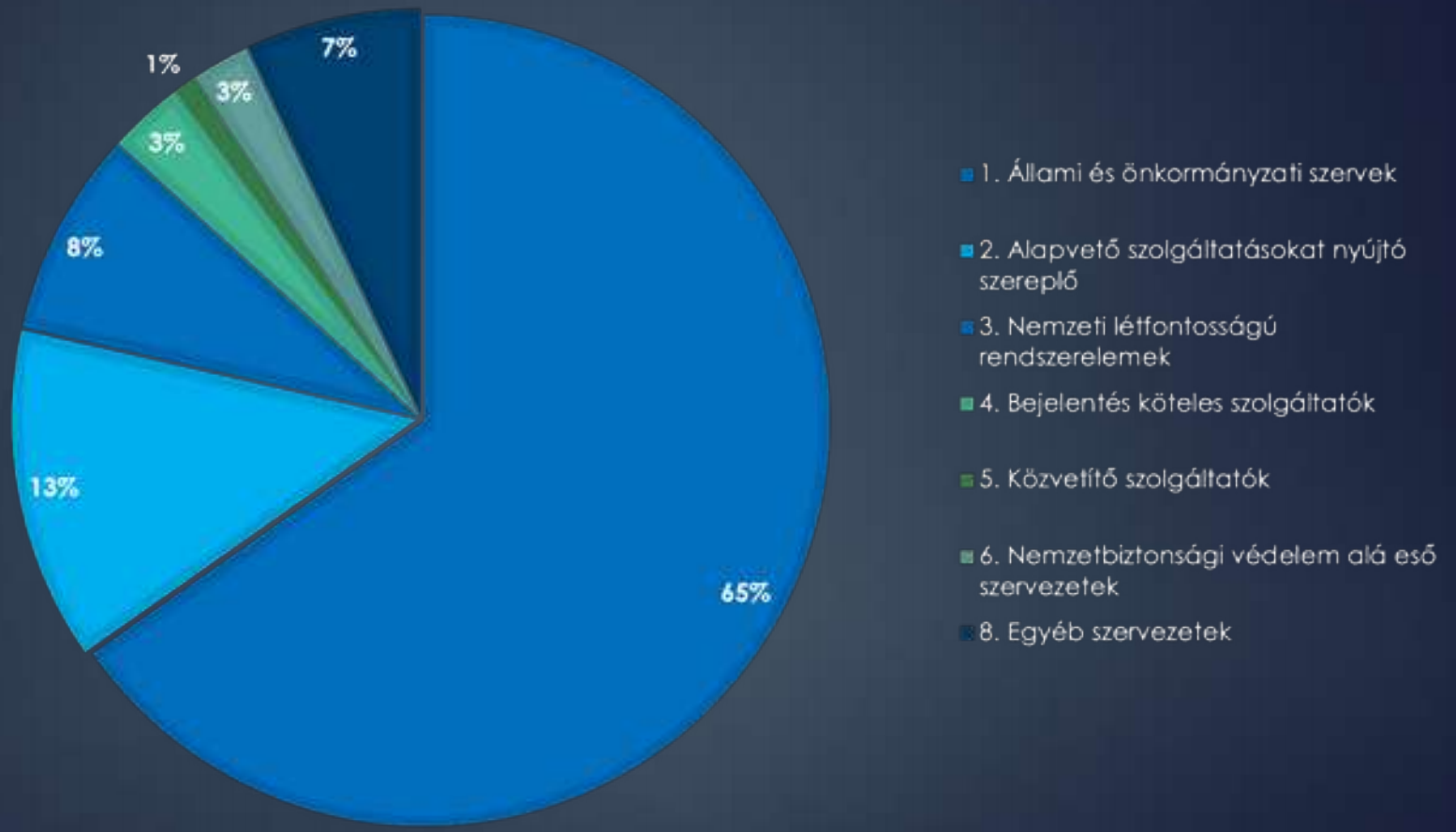
# Nemzetközi együttműködés és információmegosztás

- Koordináció az EU tagállamai között
- Közös kockázatértékelés
- Információmegosztás kötelezővé tétele

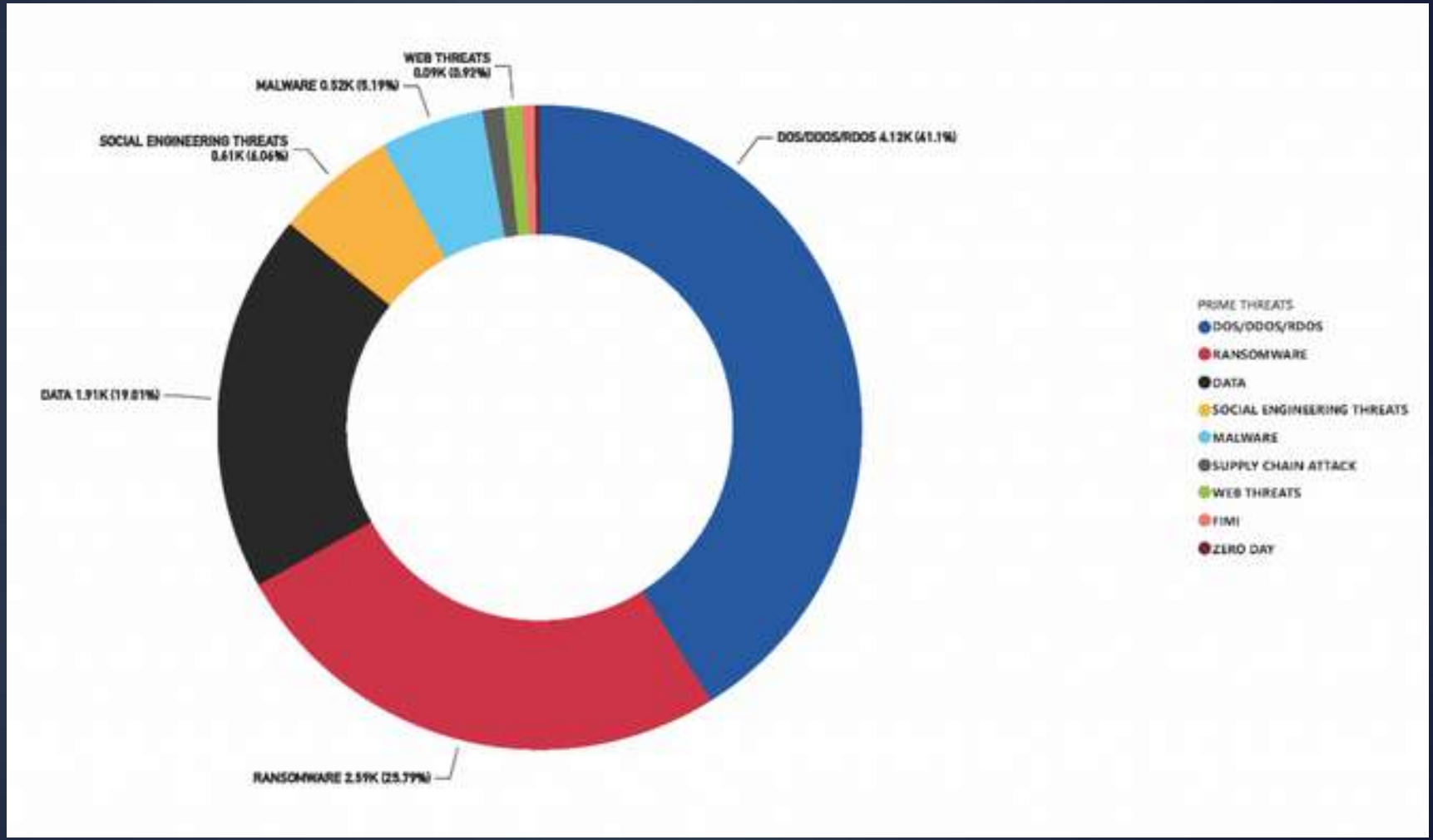
# CSIRT statisztikák

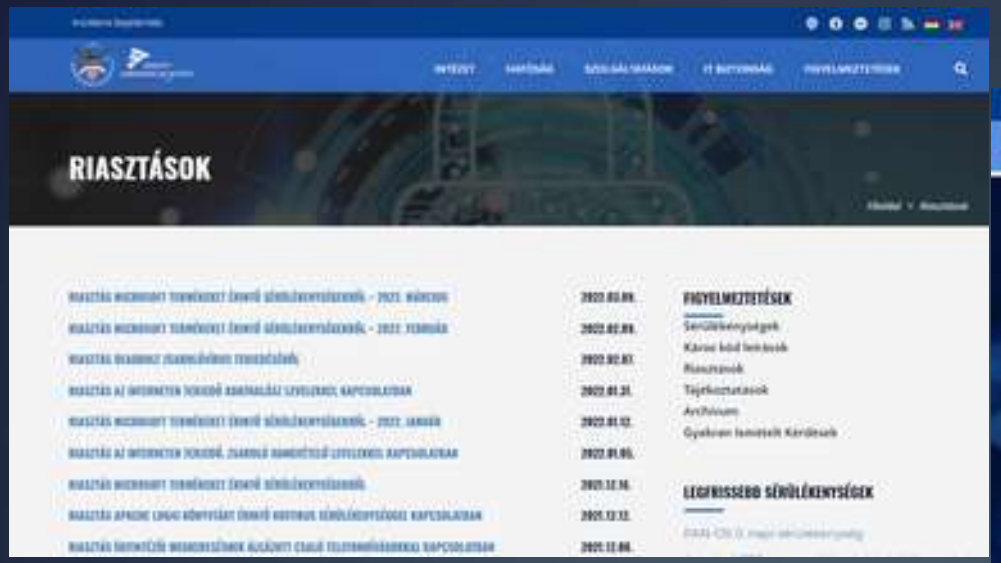


# CSIRT statisztikák



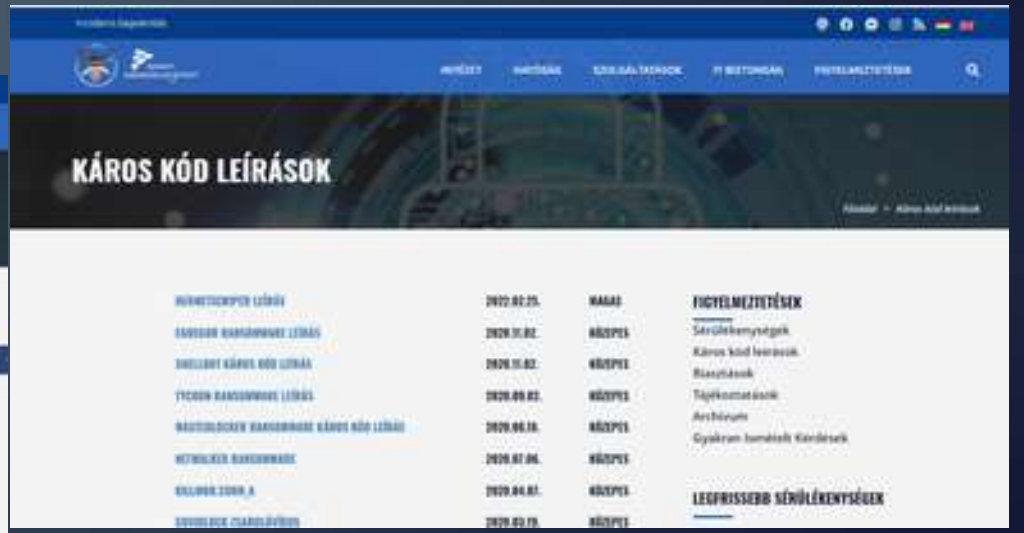
# ENISA statisztikák




RIASZTÁSOK
FIGYELMEZTETÉSEK
Sérülékenységek
Káros kód leírások
Riasztások
Tájékoztatások
Archívum
Gyakran Ismételt Kérdések
LEGFRISSEBB SÉRÜLÉKENYSÉGEK


Kiemelt témák
Jelszavak
Kéretlen levelek
Zsarolóvírus
Adathalászat
Hogyan cselezhetjük ki a QR-kódos csalókat?

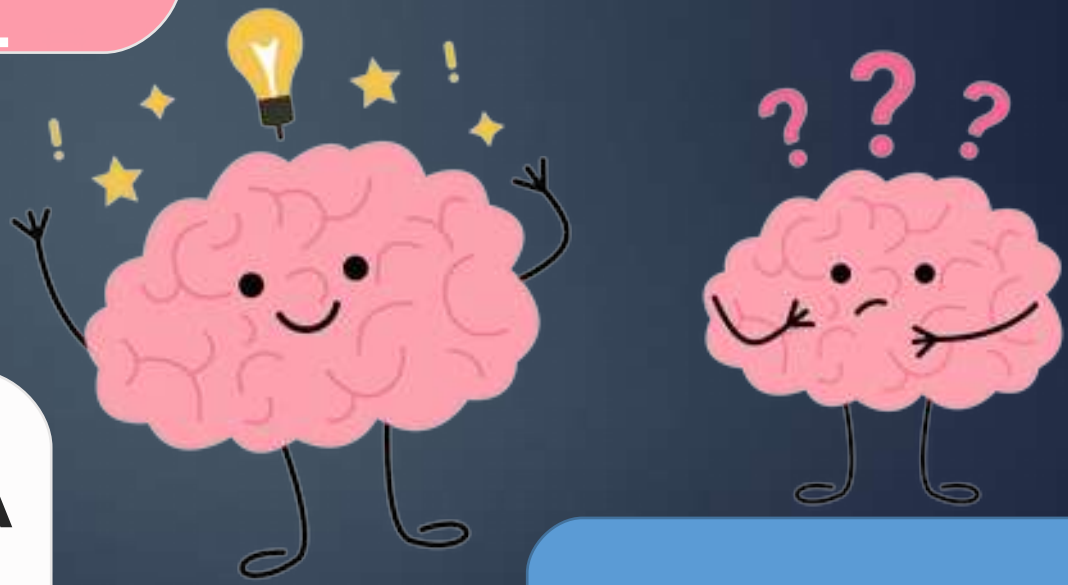

TÁJKOZTATÓ A KASPERSKY TERMÉKEK HASZNÁLATÁRÓL
FIGYELMEZTETÉSEK
Sérülékenységek
Káros kód leírások
Riasztások
Tájékoztatások
Archívum
Gyakran Ismételt Kérdések
LEGFRISSEBB SÉRÜLÉKENYSÉGEK


KÁROS KÓD LEÍRÁSOK
FIGYELMEZTETÉSEK
Sérülékenységek
Káros kód leírások
Riasztások
Tájékoztatások
Archívum
Gyakran Ismételt Kérdések
LEGFRISSEBB SÉRÜLÉKENYSÉGEK

# Hol tájékozódjak?

HASZNÁLJUNK ERŐS JELSZAVAKAT

HASZNÁJUK A KÉT FAKTOROS HITELESÍTÉST



FONTOLJUK MEG A JELSZÓSZÉF HASZNÁLATÁT

NE HASZNÁLJUK ÚJRA A

# Köszönöm a figyelmet!

*tamas.marsi@nki.gov.hu*

Kibertámadás! podcast

LinkedIn

nki.gov.hu

NEMZETI KIBERVÉDELMI INTÉZET