Tikos Anita I Vezető felügyelő

EIVOK-34. Információbiztonsági Szakmai Fórum
2023.03.30.

DORA RENDELET ELŐÍRÁSÁNAK ÉS IMPLEMENTÁCIÓJÁNAK BEMUTATÁSA

DORA RENDELET ELŐZMÉNY, MEGJELENÉS

Előzmények 2019:

2019 ESAs joint technical advice

2019 december: társadalmi konzultáció

Digitális Pénzügyi Csomag (DFP):

2020. szeptember

- Markets in Crypto-Assets (MiCA)
- DLT Pilot Regime
- **Digital Operational Resilience Act (DORA)**

DORA végleges szövegének elfogadása
2022. június 29-30.

Megjelent az EU hivatalos lapban:
2022. december 27.

RENDELET CÉLJA

- Széttöredezett szabályozási keretrendszer egyesítése, egységes terminológia
- Incidensjelentési kötelezettségek egységesítése/bevezetése
- A harmadik fél szolgáltatókkal kapcsolatos kockázatok kezelése
- A legnagyobb és legkritikusabb szolgálatók EU-s szintű felvigyázása
- NIS2 irányelvhez (2022/2555 számú irányelv) szektorspecifikus lex specialis
- Arányosság elve szerinti alkalmazás

Forrás | MNB

NIS2 IRÁNYELV (2022/2555 SZÁMÚ)

DORA-t ágazatspecifikus jogi aktusnak kell tekinteni:

IKT kockázatkezelés, jelentéstétel, felügyelet és végrehajtás tekintetében

Hatály:

- Banki szolgáltatások
- Pénzügy piaci infrastruktúrák
- *Digitális infrastruktúrák:*
  - *felhő szolgáltatók,*
  - *adatközpont szolgáltatók*
- *IKT szolgáltatások irányítása (vállalkozások)*

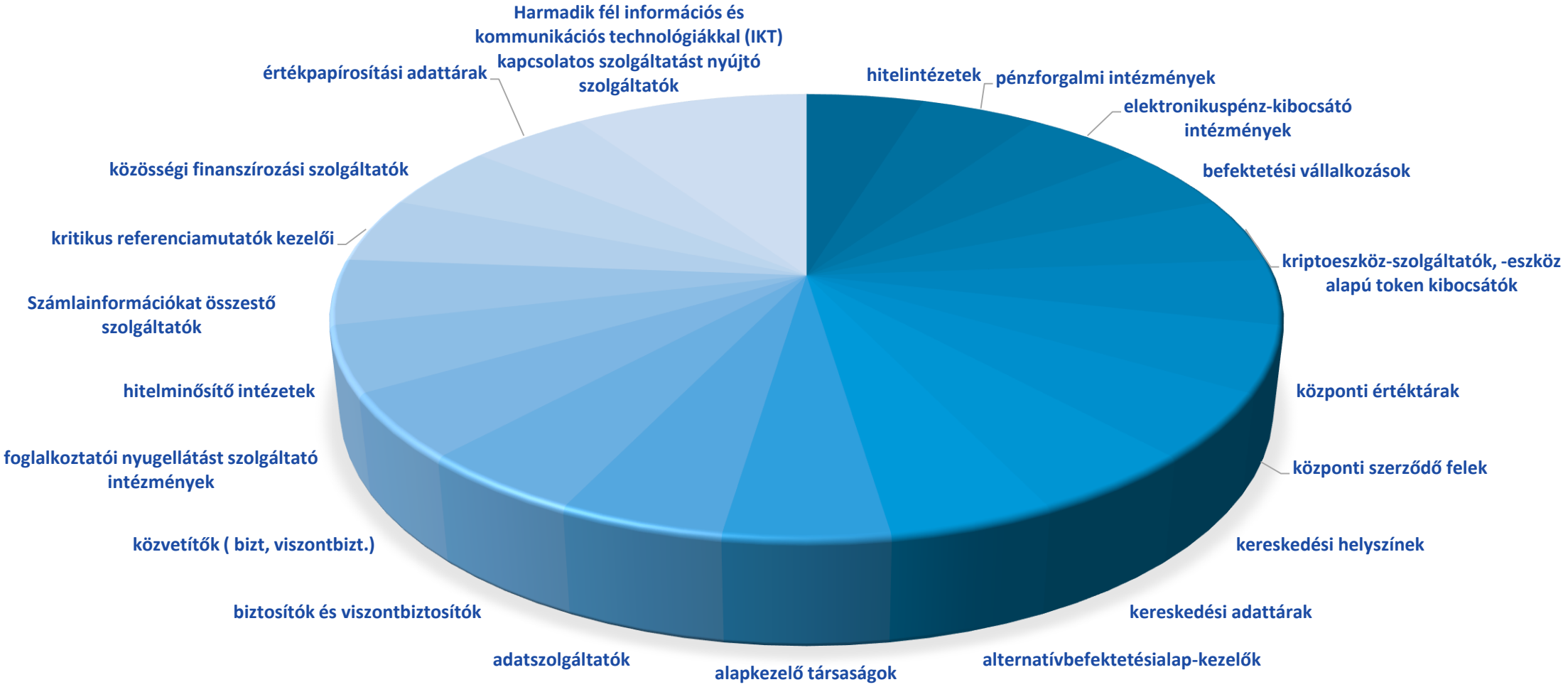
Kockázatkezelés:

alapelvi szintű szabályozás

Incidensek:

- Jelentős esemény: 3 szintű (korai: észlelést követő 24 órán belül, időközi 27 órán belül, záró korai jelzéshez képest 1 hónap)
- Majdnem bekövetkezett események és kiberfenyegetések

DORA HATÁLYA



Forrás | MNB

DORA RENDELET FELÉPÍTÉSE

- **IKT-kockázatkezelés**
- IKT-vonatkozású események kezelése, osztályozása, bejelentése
- Digitális működési ellenállóképesség **tesztelése**
- Harmadik féltől eredő IKT-kockázatok kezelése
- **Információmegosztásra vonatkozó megállapodások**
- **Illetékes hatóságok**

Forrás | MNB

IKT-VONATKOZÁSÚ BIZTONSÁGI ESEMÉNYEK

Kezelés

- Egy az IKT-val kapcsolatos események nyomon követésére és naplózására alkalmas folyamat kidolgozása, alkalmazása
- **Nyilván kell tartani valamennyi IKT eseményt és jelentős kiberfenyegetést**
- **Kommunikációra vonatkozó tervek, eljárások** (média, ügyfelek, szolgáltatók, belső eszkaláció)

Osztályozás

- Az **IKT vonatkozású incidensek osztályozása** megadott kritériumrendszer szerint (a későbbi RTS-ben meghatározott küszöbértékek alapján)
- **Fenyegetések osztályozása**

Bejelentés

- **Az incidensek bejelentése az NCA-knak** az ESA-k által kidolgozandó egységes űrlapok alkalmazásával;
  - jelentős IKT események
  - jelentős pénzforgalmi vonatkozású működési vagy biztonsági események
  - jelentős kiberfenyegetések (önkéntes alapú)

Jelentős kiberfenyegetéssé minősítés szempontjai:

A kockázatnak kitett szolgáltatások kritikussága alapján, ideértve a pénzügyi szervezet ügyleteit és műveleteit, a megcélzott ügyfelek vagy pénzügyi partnerek számát és/vagy relevanciáját, valamint a kockázatnak kitett területek földrajzi eloszlását.

Forrás I MNB

FENYEGETÉS ALAPÚ BEHATOLÁSI TESZTELÉSE (TLPT)

- olyan keret, amely utánozza egy tényleges kiberfenyegetés forrásának tekintett, valós fenyegetést jelentő szereplők taktikáját, módszereit és eljárásait, és amely **elvégzi a pénzügyi szervezet kritikus éles rendszereinek kontrollált, testreszabott, hírszerzésen alapuló (red team) tesztelését**
- **nagyon komplex, idő és humánerőforrás igényes teszt**
- 3 évente
- az illetékes hatóságok által (megadott szempontok szerint) kiválasztott intézmények
- A tesztelőkre vonatkozó követelmények (27. cikk)

HARMADIK FÉLTŐL EREDŐ IKT-KOCK. KEZELÉS

IKT-szolgáltatások: IKT-rendszerek útján egy vagy több belső vagy külső felhasználó részére **folyamatos jelleggel nyújtott digitális és adatszolgáltatások,** ideértve a hardvert mint szolgáltatást és a hardverszolgáltatásokat, ami magában foglalja a hardverszolgáltató általi szoftver- vagy belsőrendszervezérlőprogram-(firmware-) frissítéseket is, ide nem értve a hagyományos analóg telefonszolgáltatásokat

IKT harmadik fél szolgáltatók (TPP) kockázatainak kezelésének harmonizálása	TPP-vel kötendő szerződéses megállapodások	Uniós felvigyázói keretrendszer a kritikus IKT harmadik fél szolgáltatókra vonatkozóan
TPP IKT-kockázatra vonatkozó stratégia, Minimum követelmények Kockázatok folyamatos monitorozása	**Főbb alapelvek** (intézmény felelőssége, dokumentáció) **Nyilvántartás (RoI)** **szerződéses követelmények**	Felvigyázók: ESA-k NCA: felvigyázás támogatása, JET, közvetítés az intézmények felé

A RENDELETBŐL ADÓDÓ FELADATOK ÜTEMEZÉSE

Alkalmazandó: 2025. január 17.

EU-s feladatok: JC SC DOR

12 hónap

- **IKT kockázatkezelési keretrendszer (RTS)**
- **Egyszerűsített IKT kockázatkezelési keretrendszer (RTS)**
- **IKT szolgáltatásokra vonatkozó szabályzati elvárások meghatározása (RTS)**
- **IKT vonatkozású események osztályozásának kritériumai (RTS)**
- **IKT harmadik fél szolgáltatókról szóló nyilvántartás űrlapja (ITS)**

18 hónap

- **TLPT teszt aspektusainak specifikációja (RTS)**
- **Kritikus vagy fontos funkciók esetén alvállalkozók alkalmazásának feltételei (RTS)**
- **IKT vonatkozású események bejelentési szabályai (RTS)**
- **IKT vonatk. események bejelentésének tartalma (ITS)**
- **A jelentős IKT vonatk. események okozta kár/költség megbecslésének módja (GI.)**
- ESAk és a tagállami hatóságok közötti együttműködés a felvigyázási struktúrában (GI.)
- A felvigyázói tevékenységgel kapcsolatos feltételek/információk harmonizálása (RTS)

24 hónap

- Megvalósíthatósági tanulmány az IKT vonatkozású események központosított EU-s bejelentési felületére

Nemzeti feladatok:

Nem átültetendő, de kell jogharmonizáció

MNB informatikai ajánlásainak és az ágazati jogszabályok felülvizsgálata

DORA szerinti adatszolgáltatások, űrlapok bevezetése

Forrás | MNB

ESA ELŐÍRÁSOK HARMONIZÁCIÓJA

EBA:

- Iránymutatások a felügyeleti felülvizsgálati és értékelési eljárás (SREP) során végzendő IKT-kockázat értékeléshez
- Iránymutatások az IKT- és biztonsági kockázatok kezelésére
- Iránymutatás a kiszervezésről

EIOPA:

- Az információs és kommunikációs technológiák biztonságára és irányítására vonatkozó iránymutatások
- Iránymutatások a felhőszolgáltatókhoz történő kiszervezésről

ESMA:

- Guidelines on outsourcing to cloud service providers

Felülvizsgálatukról szóló diskurzus 2024 második felében várható

KÖSZÖNÖM SZÉPEN A FIGYELMET!

Anita TIKOS
vezető felügyelő

1122 Bp., Krisztina krt.6.
Telefon: +36-1- 489-9753
Email: tikosa@mnb.hu

Forrás I MNB