NIS 2 IMPLEMENTÁCIÓJA

2023. október 3.

Selyem Zsuzsanna
NBSZ NKI Hatósági Főosztály
zsuzsanna.selyem@nki.gov.hu

ALAPVETÉSEK

jogszabályok felülvizsgálatának célja: NIS 2 implementáció + Ibtv. elmúlt 10 év tapasztalatai

az implementációs határidő:

- 2024. október 17.

hatályba lépés:

- 2024. október 18.

ELŐKÉSZÍTŐ TEVÉKENYSÉG

Nemzeti Kiberbiztonsági Koordinációs Tanácson belül:

NIS 2 munkacsoport

NIS 2 munkacsoport keretében 4 alcsoport:

- hatósági
- sérülékenység-vizsgálati
- eseménykezelési
- válságkezelési

tervezés:

- 2023. 09-10.hó: munkacsoporti előkészítő egyeztetések lefolytatása
- 2024. 01-02.14: jogszabályszöveg szakmai egyeztetése munkacsoport keretében
- 2024. 02. 29.: közigazgatási egyeztetésre kiküldés

munkacsoporti tevékenység keretében:

- egyeztetés előtt: előkészítő anyag kiküldés
- egyeztetést követően: írásos észrevételek, javaslatok jelzése 5 munkanapon belül

NIS 2 hatálya

A NIS 1-hez képest, hogy a NIS 2 irányelv hatálya jóval **több ágazatra terjed ki,** a NIS 1 tág jogkört biztosított a tagállamoknak – a NIS 2 kiküszöböli ezt a problémát, a tagállami azonosítás helyett méretkorlátot vezet be.

Kibővült az irányelv hatálya alá került ágazatok száma, melyet az Irányelv melléklete két csoportra oszt:

kiemelten kritikus ágazatok (sok egyezés a NIS 1-el, mely tovább bővül pl. közigazgatás, világűr)

egyéb kritikus ágazatok
(pl. postai futárszolgálatok, élelmiszer termelés, digitális szolgáltatók)

Az irányelvben foglalt kötelezettségek alkalmazásának - az adott ágazatba tartozás mellett - egyéb feltételei is lehetnek, például az, hogy egy bizonyos méretet elérjenek az érintett szolgáltatók (lásd NIS 2 Irányelv 2. cikk (1) bek.)

A JÖVŐ

4 kiberbiztonsági hatóság:

- NIS 2: SZTFH
- NIS 2 közigazgatás ágazat és kritikus szervezetek (kivéve DORA): NBSZ
- DORA: MNB
- honvédelmi ágazat: KNBSZ

a törvény hatálya megbontásra kerül:

- felügyelet (hatóság)
- sérülékenységvizsgálat
- eseménykezelés

HATÓSÁGI HATÁLY

jelentősebb változások:

- alapvető és fontos szervezetek megkülönböztetése (kisebb önkormányzati hivatalok a fontos szervezetek közé)
- központi szolgáltatók és a központi rendszerek szolgáltatói nevesítetten a hatály alá kerülnek
- többségi állami befolyás alatt álló gazdasági társaságok bevonása
- a hatósági azonosítás lehetősége alapvető és fontos szervezetként

ESEMÉNYKEZELÉSI HATÁLY

jelentősebb változások:

- hatósági ügyfelek
- KibertanTv. alá tartozók
- DORA rendelet alá tartozók
- önkéntes bejelentők

- ágazati eseménykezelő központok

SÉRÜLÉKENYSÉGVIZSGÁLATI HATÁLY

jelentősebb változások:

EGYEZTETÉS ALATT!

- sérülékenységvizsgálat / ASR különböző
- hatósági ügyfelek
- állami vagy uniós forrásból fejlesztett rendszerek
- sérülékenységvizsgálatot végző gazdálkodó szervezetek nyilvántartása → NBSZ NKI

ÚJ, MEGVÁLTOZOTT FOGALMAK

ipari rendszer, központi rendszer, központi rendszer szolgáltatója, központi szolgáltató, végfelhasználó, szervezet rendelkezésében lévő EIR, kiberfenyegetés, kibertámadás, majdnem bekövetkezett (near miss) incidens, incidens, jelentős incidens, nagyszabású kiberbiztonsági incidens, incidenskezelés stb.

BIZTONSÁGI OSZTÁLY ÉS ~~-SZINT~~

biztonsági szintbe sorolás kivezetése

biztonsági osztályba sorolás

- biztonsági osztályoknál 3 fokozatú skála: alap, jelentős, magas
- összhang a kiberbiztonsági tanúsítási rendszerrel és a követelményrendszer alapját képező NIST 800-53-al

ÚJ ELEMEK

- fejlesztések szigorúbb felügyelete (belső és/vagy hatósági engedélyezés)
- kiberválságkezelés (EU-CyCLONe)
- kötelező gyakorlatok
- követelményrendszer megújítása

KÖVETELMÉNYRENDSZER I.

alapja: NIST 800-53 rev.5

- külön **felhő és OT** követelményrendszer
- 3 kategória
- kockázatelemzés alapján testreszabható
- intézkedések csoportosítása változik (adminisztratív, fizikai, logikai helyett kontroll családok szerint)
- intézkedések BSR besorolása megszűnik

KÖVETELMÉNYRENDSZER II.

Köszönöm a figyelmet!