# Kiberbiztonsági feladatok *és változások*

Szabó Lajos · Nemzeti Kiberbiztonsági Intézet · igazgató

# Egy évvel *később*

- Az új követelmények alkalmazása napi feladat lett.
- További szabályok léptek életbe.
- Új tapasztalatokat szereztünk az AI kiberbiztonsági képességeiről.

A szolgáltatásokat közben folyamatosan fenn kell tartani.

# A korábbi döntések szerepe *az incidensekben*

- Milyen rendszert szereztünk be?
- Milyen hozzáférést adtunk a szolgáltatónak?
- Ismertük-e a külső komponenseket?
- Egyértelmű volt-e, ki kezeli a biztonsági jelzéseket?

A biztonsággal már a fejlesztés, a beszerzés és az üzemeltetés tervezésekor számolni kell.

# A CRA jelentéstételi *kötelezettségei*

- 2026. szeptember 11-től egyes jelentéstételi kötelezettségek.
- 2027 decemberétől a fő követelmények.

A gyártóknak rövid határidőn belül jelenteniük kell:

- az aktívan kihasznált sérülékenységeket,
- a termékeik biztonságát érintő súlyos incidenseket.

# Teendők a sérülékenység *bejelentése után*

Tudnunk kell, érintettek vagyunk-e, és mit kell tennünk.

- Naprakész nyilvántartás.
- Ismert kapcsolattartó.
- Kipróbált frissítési eljárás.

Ehhez a gyártónak, a szolgáltatónak és a felhasználónak együtt kell működnie.

# Az AI-ügynökökkel *végzett tesztek tapasztalatai*

Kutatási tesztek során egyes AI-ügynökök a vizsgálat körén kívüli éles rendszerekhez is hozzáfértek.

- A tesztekben bizonyos védelmi korlátozásokat szándékosan feloldottak.
- Az AI-ügynökök összetett műveletsorokat hajtottak végre, kevés emberi beavatkozással.
- Számolnunk kell azzal, hogy ezeket a képességeket támadók is felhasználhatják.

# Az AI-ügynökök *használata a szervezetben*

**Előre meghatározott keretek**

- Engedélyezett hozzáférések és önálló műveletek.
- Emberi jóváhagyás.
- Követhető működés, szükség esetén leállítható folyamatok.

**AI a védekezésben**

- Segítheti a sérülékenységfeltárást és az elemzést.
- Automatizálhatja az ismétlődő feladatokat.
- A több feltárt hibához megfelelő ellenőrzési és javítási kapacitás kell.

# A Nemzeti Kiberbiztonsági Ügynökség *létrehozásának terve*

**A közzétett célok**

- A feladatköri szabályozások átalakítása.
- Új eljárások kialakítása.
- Független státuszú szervezet felállítása.

**Az eredmény megítélésének szempontjai**

- Érthetőbb elvárások.
- Könnyebb együttműködés.
- Gyorsabb szakmai segítség.
- Egyértelmű feladat- és felelősségi körök.
- A biztonsági információk eljuttatása az intézkedésért felelősökhöz.

# *Köszönöm a figyelmet!*

Szabó Lajos
lajos.szabo@nki.gov.hu
+ 36 30 512 6492