Jelentés a kiberbiztonság helyzetéről az Európai Unióban –
2024 Report on the State of the Cybersecurity in the Union
ENISA – European Union Agency for Cybersecurity, December 2024 (20 p.) ;
Apud EGOV Hírlevél. Közigazgatás& Informatika, 2024. december 8.

Kulcsszavak: európai egészségügy, egészségügyi informatika, kiberbiztonság, Európai Unió

Forrás Internet-helye: https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union ;
https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20Cybersecurity%20in%20the%20Union%20-%20Condensed%20version.pdf ;
https://hirlevel.egov.hu/2024/12/08/megjelent-az-unios-kiberbiztonsagi-ugynokseg-enisa-elso-jelentese-a-kiberbiztonsag-helyzeterol-az-unioban/

„A NIS 2 irányelv 18. cikkével összhangban az ENISA-t azzal bízták meg, hogy kétévente készítsen jelentést a kiberbiztonság helyzetéről az Unióban.

A jelentés bizonyítékokon alapuló áttekintést nyújt a kiberbiztonság érettségi szintjéről, valamint értékeli a kiberbiztonsági képességeket Európa-szerte. A jelentés szakpolitikai ajánlásokat is tartalmaz a feltárt hiányosságok orvoslására és az EU kiberbiztonsági szintjének növelésére.

Az elvégzett elemzés különböző forrásokon alapul, többek között az ***EU Cybersecurity Index***-en, a ***NIS Investment*** jelentéssorozaton, a ***Foresight 2030***-on és az ***ENISA Threat Landscape*** jelentésen. A munka mind a 27 uniós tagállammal és az Európai Bizottsággal folytatott széles körű konzultáció eredménye.

A főbb megállapítások

Az uniós szintű kockázatértékelés szerint jelentős az EU-t érintő kiberfenyegetettség szintje, kiemelendők a felfedezett sebezhetőségek, amelyeket az uniós jogalanyokat célzó fenyegető szereplők kihasználnak.

Ami az uniós szintű kiberbiztonsági képességeket illeti, az uniós tagállamok olyan kiberbiztonsági stratégiákat dolgoztak ki, amelyek céljai összességében összhangban vannak egymással. A kritikus ágazatok méretük és kritikusságuk tekintetében heterogénebbnek tűnnek, ami megnehezíti a kiberbiztonsági intézkedések felügyeletét és egységes végrehajtását. A polgárok szintjén a jelentés azt feltételezi, hogy az uniós polgárok körében valószínűleg nőtt a kiberbiztonsági tudatosság. A fiatalabb generációk digitális készségeinek szintje magasabbnak tűnik, annak ellenére, hogy az oktatási programok elérhetősége és az oktatás érettsége tagállamonként eltérő.

Szakpolitikai ajánlások

A jelentés **négy kiemelt területet** határoz meg, amelyekkel a szakpolitikai ajánlások foglalkozniuk kell: 1) szakpolitika végrehajtása, 2) kiberválságkezelés, 3) ellátási lánc és 4) készségek.

A jelentés legfontosabb eredménye hat szakpolitikai ajánlás, amelyek a fenti négy kiemelt területre, valamint a kritikus szektor szereplőinek képességeire, a kiberbiztonsági tudatosságra és a kiberhigiéniára terjednek ki.

- Az Európai Unió intézményei, szervei és ügynökségei (EUIBA-k), az illetékes nemzeti hatóságok és a NIS2 irányelv hatálya alá tartozó szervezetek számára nyújtott technikai és pénzügyi támogatás megerősítése a **kialakuló uniós kiberbiztonsági szakpolitikai keret összehangolt, átfogó, időben történő és koherens végrehajtásának biztosítása** érdekében, a már meglévő uniós szintű struktúrák, például a NIS együttműködési csoport, a CSIRT-hálózat és az uniós ügynökségek felhasználásával.
- A Tanács felkérésének megfelelően a **nagyszabású kiberincidensekre való összehangolt reagálásra vonatkozó uniós terv felülvizsgálata**, figyelembe véve az EU legújabb kiberbiztonsági szakpolitikai fejleményeit. A felülvizsgált uniós tervnek továbbá **elő kell mozdítania az uniós kiberbiztonsági harmonizációt és optimalizálást**, valamint **meg kell erősítenie mind a nemzeti, mind az uniós kiberbiztonsági képességeket** a nemzeti és európai szintű kiberbiztonsági ellenálló képesség fokozása érdekében.
- Az **uniós kiberbiztonsági munkaerő megerősítése** a ***Cybersecurity Skills Academy*** létesítésével, különösen a **kiberbiztonsági képzésre vonatkozó közös uniós megközelítés** kialakításával, a jövőbeli készségigények meghatározásával, a **készséghiány kezelése** érdekében az **érdekelt felek bevonásával kapcsolatos összehangolt uniós megközelítés** kidolgozásával és a **kiberbiztonsági készségek európai tanúsítási rendszerének** létrehozásával.
- Az ellátási lánc biztonságának kezelése az EU-ban az **egész EU-ra kiterjedő összehangolt kockázatértékelések fokozásával** és az **ellátási lánc biztonságára vonatkozó uniós horizontális politikai keret** kidolgozásával, amelynek célja az állami és a magánszektor előtt álló kiberbiztonsági kihívások kezelése. Az ágazati és a magánszektorok biztonságának fokozottabb megértése.
- **Az ágazati sajátosságok és szükségletek jobb megértése, a NIS2-irányelv hatálya alá tartozó ágazatok kiberbiztonsági érettségi szintjének javítása. A kiberbiztonsági szolidaritásról szóló törvény (*Cyber Solidarity Act*) alapján létrehozandó jövőbeli kiberbiztonsági vészhelyzeti mechanizmus (*Cybersecurity Emergency Mechanism*)** felhasználása az ágazati felkészültség és ellenálló képesség érdekében, különös tekintettel a gyenge vagy érzékeny ágazatokra és az uniós szintű kockázatértékelések révén azonosított kockázatokra.
- Az **egységes megközelítés** előmozdítása a meglévő szakpolitikai kezdeményezésekre építve és a nemzeti erőfeszítések összehangolásával annak érdekében, hogy a szakemberek és a polgárok körében – demográfiai jellemzőktől függetlenül – **közös, magas szintű kiberbiztonsági tudatosságot és kiberhigiéniát** érjenek el.