2024/1101

2024.4.12.

A BIZOTTSÁG (EU) 2024/1101 AJÁNLÁSA

(2024. április 11.)

a posztkvantum-kriptográfiára való átállás összehangolt végrehajtási ütemtervéről

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 292. cikkére,

tekintettel az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről szóló, 2022. december 14-i (EU) 2022/2555 európai parlamenti és tanácsi irányelvre ([1]) (NIS 2 irányelv),

mivel:

(1) Az adatok védelme és az érzékeny kommunikáció biztonságos volta létfontosságú az Unió társadalma, gazdasága, biztonsága és jóléte szempontjából. A kiberbiztonság stratégiai fontosságú a digitális korra felkészült Európa építésében ([2]), és a Digitális évtized szakpolitikai program ([3]) egyik fő célkitűzése.

(2) A biztonsági unióra vonatkozó uniós stratégia ([4]) és az uniós kiberbiztonsági stratégia ([5]) egyaránt kiemeli, hogy a titkosítás kulcsfontosságú technológia a reziliencia és a technológiai szuverenitás megvalósításához, valamint a kibertámadások megelőzéséhez szükséges operatív kapacitás kiépítéséhez. A titkosítás ugyanis alapvető fontosságú a digitális világban a digitális rendszerek és tranzakciók biztonsága, az alapvető jogok védelme, valamint a védelmi képességek biztosítása szempontjából. A különböző országok és magánszervezetek által a kvantumszámítástechnikai képességek fejlesztése és a potenciálisan előnyös új lehetőségek kiaknázása érdekében folytatott verseny fenyegetést jelent a jelenlegi kriptográfiai szabványokra nézve. E szabványok kulcsszerepet játszanak az adatok bizalmas jellegének és integritásának biztosításában, az érzékeny kommunikáció védelmében, valamint a hálózatbiztonság alapvető elemeinek támogatásában.

(3) A mai titkosítás feltörésére képes kvantumszámítógépek jövőbeli potenciális fejlődése szükségessé teszi, hogy Európa erősebb biztosítékokat keressen, biztosítva az érzékeny kommunikáció védelmét és a bizalmas információk hosszú távú integritását, ami a posztkvantum-kriptográfiára való lehető leggyorsabb áttérést jelenti. Ez az új típusú kriptográfia megszünteti a jelenlegi, nyilvános kulcsú kriptográfia ismert sebezhetőségeit, és fokozza a kvantumszámítógépek rosszindulatú használatából eredő fenyegetésekkel szembeni ellenálló képességet.

(4) A Bizottság több mint egy évtizede finanszírozza a posztkvantum-kriptográfiára irányuló kutatást és fejlesztést, elismerve, hogy a kvantuminformatika veszélyt jelenthet a jelenleg alkalmazott nyilvános kulcsú kriptográfiára.

(5) A tagállamoknak fontolóra kell venniük, hogy a közigazgatások és más kritikus infrastruktúrák által jelenleg használt digitális infrastruktúráikat és szolgáltatásaikat korszerűsítsék posztkvantum-kriptográfiára, ami alapvető elmozdulást eredményezne a kriptográfiai algoritmusok, protokollok és rendszerek terén. Amint azt a Bizottság nemrégiben kiadott, „Hogyan kezeljük Európa digitális infrastrukturális igényeit?” című fehér könyve is kiemelte, ehhez összehangolt erőfeszítésekre van szükség a kormányzati ügynökségek, a szabványügyi testületek, az ágazati érdekelt felek, a kutatók és a kiberbiztonsági szakemberek bevonásával.

(6) Ez a bizottsági ajánlás arra ösztönzi a tagállamokat, hogy dolgozzanak ki átfogó stratégiát a posztkvantum-kriptográfia bevezetésére a különböző tagállamokban és állami szektoraikban megvalósítandó összehangolt és szinkronizált átállás biztosítása érdekében. A stratégiának egyértelmű célokat, mérföldköveket és határidőket kell meghatároznia, amelyek eredményeként közös posztkvantum-kriptográfiai végrehajtási ütemterv kerül

([1]) HL L 333., 2022.12.27., 80. o.
([2]) COM(2020) 67 final.
([3]) Az Európai Parlament és a Tanács (EU) 2022/2481 határozata (2022. december 14.) a Digitális évtized 2030 szakpolitikai program létrehozásáról (HL L 323., 2022.12.19., 4. o.).
([4]) COM(2020) 605 final.
([5]) JOIN(2020) 18 final.

meghatározásra. Ennek azt kell eredményeznie, hogy a posztkvantum-kriptográfiai technológiákat az egész Unióban bevezetik a meglévő közigazgatási rendszerekbe és kritikus infrastruktúrákba olyan hibrid rendszereken keresztül, amelyekben a posztkvantum-kriptográfia kombinálható a meglévő kriptográfiai megközelítésekkel vagy a kvantumalapú kulcsszétosztással.

(7) A posztkvantum-kriptográfiára való hatékony átállás érdekében az összehangolt posztkvantum-kriptográfiai végrehajtási ütemtervnek tartalmaznia kell a tagállamok által végrehajtandó intézkedések listáját – beleértve a posztkvantum-kriptográfiai algoritmusok mérlegelését – a különböző szakaszok és mérföldkövek egyértelmű ütemezésével, figyelemmel azok kölcsönös függőségeire, valamint a bevonandó érdekelt feleket.

(8) A posztkvantum-kriptográfia Unió-szerte történő harmonizált alkalmazása érdekében alapvető fontosságú a közös európai szabványok kidolgozása, valamint a digitális hálózatokban és szolgáltatásokban Unió-szerte bevezetendő posztkvantum-kriptográfiai algoritmusok azonosítására és kiválasztására szolgáló keret kidolgozása. Az uniós finanszírozású kutatók aktív részvétele révén az Unió már jelenleg is támogatja az esetlegesen szabványként használható posztkvantum-kriptográfiai algoritmusok kidolgozását és tesztelését a nemzetközi posztkvantum-kriptográfiai kiválasztási folyamatokban. Az Unió-szerte harmonizált végrehajtás érdekében ez a bizottsági ajánlás arra ösztönzi a tagállamokat, hogy uniós szinten szorosan működjenek együtt az Unió kiberbiztonsági szakértőivel, a Kiberbiztonsági Együttműködési Csoporttal és az Európai Uniós Kiberbiztonsági Ügynökséggel (ENISA) a megfelelő posztkvantum-kriptográfiai algoritmusok értékelése és kiválasztása, valamint azok uniós szabványként való elfogadása terén.

(9) A kommunikáció interoperabilitásának biztosítása érdekében a tagállamoknak és az Uniónak továbbra is aktívan együtt kell működniük nemzetközi stratégiai partnereikkel a posztkvantum-kriptográfiára vonatkozó nemzetközi szabványok kidolgozásában.

(10) A tagállamok általi elfogadását követően az összehangolt posztkvantum-kriptográfiai végrehajtási ütemtervnek mintaként kell szolgálnia a posztkvantum-kriptográfiára való nemzeti átállási tervek meghatározásához, illetve – amennyiben már léteznek ilyen nemzeti tervek – azoknak a közös összehangolt posztkvantum-kriptográfiai végrehajtási ütemtervvel való harmonizálásához.

(11) Annak biztosítása érdekében, hogy ezen ajánlás célkitűzései tekintetében előrelépés történjen, a Bizottság szorosan nyomon kívánja követni az ajánlásra válaszul hozott intézkedéseket. A Bizottság ezért arra ösztönzi a tagállamokat, hogy a szóban forgó nyomon követés biztosítása érdekében a Bizottság kérésére nyújtsanak be minden olyan releváns információt, amely észszerűen elvárható tőlük. Az így szerzett információk és minden egyéb rendelkezésre álló információ alapján a Bizottság értékelni fogja ezen ajánlás hatásait, majd megállapítja, hogy szükség van-e további lépésekre, többek között kötelező erejű uniós jogi aktusok előterjesztésére.

(12) Ez a posztkvantum-kriptográfiáról szóló ajánlás az uniós kiberbiztonsági stratégiában a közigazgatások és más kritikus infrastruktúrák által használt uniós digitális infrastruktúrák és szolgáltatások végpontok közötti biztonságának és rezilienciájának javítására vonatkozóan meghatározott szakpolitikai célkitűzésekre épül, a digitális egységes piac és az európai gazdasági biztonsági stratégiáról szóló közös közlemény (10919/23) ([6]) célkitűzéseit szolgálja, továbbá figyelembe veszi a kritikus infrastruktúrák fizikai és kiberbiztonsági kockázatait, valamint a kvantumtechnológiákra vonatkozó, nemrégiben végzett kockázatértékelés ([7]) keretében azonosított kockázatokat. Tiszteletben tartja az alapvető jogokat, és betartja különösen az Európai Unió Alapjogi Chartájában (7., 8. és 11. cikk) és az emberi jogok európai egyezményében (8. és 10. cikk) elismert elveket, amelyek pozitív kötelezettségeket rónak a kormányokra annak érdekében, hogy minimalizálják az információkhoz való jogosulatlan hozzáférés és az információk feletti jogosulatlan ellenőrzés kockázatát, ami szükségessé teszi a kriptográfiai technológiák védelmét és előmozdítását,

([6]) https://data.consilium.europa.eu/doc/document/ST-10919-2023-INIT/hu/pdf
([7]) JOIN(2023) 20 final.

ELFOGADTA EZT AZ AJÁNLÁST:

1. HATÁLY ÉS CÉLKITŰZÉSEK

Ezen ajánlás célja, hogy előmozdítsa az Unióban a posztkvantum-kriptográfiára való átállást a közigazgatások és más kritikus infrastruktúrák által használt digitális infrastruktúrák és szolgáltatások védelme érdekében, lehetővé téve a tagállamok számára, hogy:

1. meghatározzanak egy összehangolt posztkvantum-kriptográfiai végrehajtási ütemtervet, amelynek célja, hogy a határokon átnyúló interoperabilitás biztosítása mellett koordinálja a nemzeti átállási tervek kidolgozására és végrehajtására irányuló tagállami erőfeszítéseket;

2. kiberbiztonsági szakértők segítségével támogassák a releváns posztkvantum-kriptográfiai algoritmusok értékelését és kiválasztását, valamint ezt követően az ilyen algoritmusoknak az összehangolt posztkvantum-kriptográfiai végrehajtási ütemterv részeként Unió-szerte végrehajtandó, uniós szabványként való elfogadását;

3. megfelelő és arányos intézkedéseket hozzanak az átállásra való felkészülés érdekében.

2. A POSZTKVANTUM-KRIPTOGRÁFIÁRA VALÓ ÁTÁLLÁSRA IRÁNYULÓ ÖSSZEHANGOLT VÉGREHAJTÁSI ÜTEMTERV

4. Ez az ajánlás arra ösztönzi a tagállamokat, hogy egy erre a célra létrehozott tagállami fórumon keresztül hangolják össze intézkedéseiket uniós szinten. E célból a Bizottság azt ajánlja a tagállamoknak, hogy használják ki a kiberbiztonság területén meglévő uniós szintű struktúrákat, és a Kiberbiztonsági Együttműködési Csoporton belül hozzanak létre egy alcsoportot. A szóban forgó alcsoport tagjai a nemzeti biztonsági ügynökségek képviselői és kiberbiztonsági szakértők – különösen a nemzeti kiberbiztonsági hatóságok és az ENISA szakértői – lehetnek. Az alcsoport felkérheti az érdekelt felek – például az állami szervezetek tanácsadó testületei, az ipar, a szolgáltatók és az üzemeltetők – képviselőit, hogy vegyenek részt a munkájában azzal a céllal, hogy az uniós versenyjogi szabályokkal és az uniós adatvédelmi joggal összhangban információkat gyűjtsenek és cseréljenek a közigazgatások és egyéb kritikus infrastruktúrák által használt digitális infrastruktúrák és szolgáltatások posztkvantum-kriptográfiára való átállásáról a különböző ágazatokban, erőfeszítéseiket nemzeti szinten összehangolják, és kidolgozzák az összehangolt posztkvantum-kriptográfiai végrehajtási ütemtervet.

5. A posztkvantum-kriptográfiával foglalkozó alcsoportnak megfelelő, hatékony és arányos intézkedéseket kell mérlegelnie az összehangolt posztkvantum-kriptográfiai végrehajtási ütemterv meghatározásához és kidolgozásának koordinálásához. A Bizottság arra ösztönzi a posztkvantum-kriptográfiával foglalkozó alcsoportot, hogy kezdjen megbeszéléseket más érintett szervekkel, például az Europollal, a NATO-val vagy más felekkel az erőfeszítések megkettőzésének elkerülése és az újonnan felmerülő kihívások kezelésére irányuló koherens megközelítés biztosítása érdekében.

6. Ennek érdekében a Bizottság felkéri a tagállamokat, hogy röviddel ezen ajánlás közzétételét követően az (EU) 2017/179 bizottsági végrehajtási határozatnak ([8]) megfelelően hozzanak létre egy ilyen, posztkvantum-kriptográfiával foglalkozó alcsoportot, és nevezzenek ki szakértői képviselőket, akiknek szorosan együtt kell működniük a Bizottsággal, és akiket meg kell bízni az összehangolt posztkvantum-kriptográfiai végrehajtási ütemterv meghatározásával és kidolgozásával.

7. Az összehangolt posztkvantum-kriptográfiai végrehajtási ütemtervnek ezen ajánlás közzétételét követő két év elteltével kell rendelkezésre állnia, ezt követően kerül sor az egyes tagállamok posztkvantum-kriptográfiai átállásra vonatkozó terveinek kidolgozására és további kiigazítására az összehangolt posztkvantum-kriptográfiai végrehajtási ütemtervben meghatározott elvekkel összhangban.

3. UNIÓS SZINTŰ FELLÉPÉSEK

8. Az átfogó munkát a Bizottság a tagállamok szakértő képviselőivel együttműködve rendszeresen nyomon követi és értékeli.

([8]) A Bizottság (EU) 2017/179 végrehajtási határozata (2017. február 1.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló (EU) 2016/1148 európai parlamenti és tanácsi irányelv 11. cikkének (5) bekezdése értelmében az együttműködési csoport működéséhez szükséges eljárásrend megállapításáról (HL L 28., 2017.2.2., 73. o.).

9. E célból a Bizottság felkérheti a tagállamok képviselőit, hogy nyújtsanak be minden, tőlük észszerűen elvárható, releváns információt annak érdekében, hogy biztosítható legyen a posztkvantum-kriptográfiai összehangolt végrehajtási ütemterv kidolgozása terén elért előrehaladásnak és az ezzel kapcsolatos intézkedések hatékonyságának nyomon követése.

10. Az említett, valamint minden egyéb rendelkezésre álló információ alapján a Bizottság értékelni fogja a tervezett intézkedéseket és a tagállamok képviselői hálózatának működését, majd megállapítja, hogy szükség van-e további intézkedésekre, többek között kötelező erejű uniós jogi aktusok előterjesztésére.

4. **FELÜLVIZSGÁLAT**

11. A tagállamoknak együtt kell működniük a Bizottsággal annak érdekében, hogy legfeljebb három évvel a közzétételt követően értékeljék ezen ajánlás hatásait a megfelelő további lépések meghatározása céljából. A szóban forgó értékelés elvégzése során figyelembe kell venni a nemzeti szakértők posztkvantum-kriptográfiával foglalkozó alcsoportja által végzett munka eredményét.

Kelt Brüsszelben, 2024. április 11-én.

a Bizottság részéről
Thierry BRETON
a Bizottság tagja