AJÁNLÁSOK

A BIZOTTSÁG (EU) 2019/534 AJÁNLÁSA

(2019. március 26.)

az 5G hálózatok kiberbiztonságáról

AZ EURÓPAI BIZOTTSÁG,

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

mivel:

(1) A Bizottság a hálózati technológiák 5. generációjának (5G) telepítését a jövőbeli digitális szolgáltatások egyik fő elősegítő tényezőjeként, valamint a digitális egységes piaci stratégia egyik prioritásaként ismerte el. A Bizottság elfogadta az 5G cselekvési tervet annak biztosítása érdekében, hogy az Unió 2020-tól rendelkezzen a digitális átalakulásához szükséges hálózati infrastruktúrával ([1]).

(2) Az 5G hálózatok a jelenlegi 4. generációs hálózati technológiákra fognak épülni (4G), új szolgáltatási képességeket biztosítanak, és az uniós gazdaság nagy része számára központi infrastruktúrává és katalizátorrá fognak válni. Az 5G-hálózatok kiépülésük után a belső piac működése, valamint a létfontosságú társadalmi és gazdasági funkciók – például az energia, a közlekedés, a banki szolgáltatások és az egészségügy –, továbbá az ipari ellenőrzési rendszerek fenntartása és működtetése szempontjából alapvető fontosságú szolgáltatások széles körének gerincét fogják képezni. A demokratikus folyamatok, például a választások megszervezése is egyre inkább a digitális infrastruktúrára és az 5G-hálózatokra fog támaszkodni.

(3) Számos kritikus szolgáltatásnak az 5G hálózatoktól való függése miatt a rendszerszintű és széles körű zavarok következményei különösen súlyosak lennének. Ennek következtében az 5G hálózatok kiberbiztonságának megvalósítása stratégiai fontosságú kérdés az Unió számára egy olyan időszakban, amikor a kibertámadások egyre gyakoribbakká válnak és kifinomultabbak, mint valaha.

(4) A digitális ökoszisztémát kiszolgáló infrastruktúrák egymáshoz kapcsolódó és transznacionális, illetve a szóban forgó fenyegetések határokon átnyúló jellege miatt a tagállamok egyikében bekövetkező, az 5G hálózatokat érintő jelentős sebezhetőségek és/vagy kiberbiztonsági események az Unió egészét érintenék. Ezért kell intézkedéseket hozni az 5G hálózatok egységesen magas kiberbiztonsági szintjének alátámasztására.

(5) Az uniós szintű fellépés szükségességét a tagállamok megerősítették. Az Európai Tanács 2019. március 21-i következtetéseiben várakozással tekintett az 5G hálózatok biztonságára vonatkozó egységes megközelítésre irányuló bizottsági ajánlás elé ([2]).

(6) Fontos célként kell kezelni az európai szuverenitás biztosítását, teljes mértékben tiszteletben tartva a nyitottság és a tolerancia európai értékeit ([3]). A stratégiai ágazatokba irányuló külföldi beruházások, a kritikus eszközök, technológiák és infrastruktúra felvásárlása az EU-ban, valamint a kritikus berendezések beszállítása is kockázatot jelenthetnek az EU biztonságára.

(7) Az 5G hálózatok kiberbiztonsága kulcsfontosságú az Unió stratégiai autonómiájának biztosítása szempontjából, amint azt „Az EU és Kína – stratégiai kilátások” című közös közlemény ([4]) is elismeri.

(8) Az unióbeli növekvő kínai technológiai jelenléttel kapcsolatos biztonsági fenyegetésekre vonatkozó európai parlamenti állásfoglalás arra is felhívja a Bizottságot és a tagállamokat, hogy tegyenek uniós szintű intézkedéseket ([5]).

(9) Ez az ajánlás az 5G hálózatok kiberbiztonsági kockázataival foglalkozik azáltal, hogy iránymutatást nyújt a megfelelő nemzeti szintű kockázatelemzési és -kezelési intézkedésekhez, egy összehangolt európai kockázatértékelés kidolgozásához, valamint a legjobb kockázatkezelési intézkedések közös eszköztárának kidolgozására irányuló folyamat kialakításához.

(10) Az elektronikus hírközlő hálózatok védelmének uniós jogi kerete erős.

([1]) COM(2016) 588 final.
([2]) Az Európai Tanács 2019. március 21–22-i következtetései.
([3]) Az Unió helyzete (2018) – Elérkezett az európai szuverenitás ideje, 2018. szeptember 12.
([4]) JOIN (2019) 5 final.
([5]) www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0156+0+DOC+PDF+V0//HU.

(11) Az elektronikus hírközlés ([6]) területére vonatkozó uniós keret előmozdítja a versenyt, a belső piacot és a végfelhasználói érdekeket, és az Európai Elektronikus Hírközlési Kódexszel ([7]) együtt egy, az elért eredmények tekintetében megfogalmazott további összeköttetési célkitűzéssel is rendelkezik: széles körű hozzáférés a nagyon nagy kapacitású helyhez kötött és mobil internetkapcsolatokhoz és ezek igénybevétele valamennyi uniós polgár és vállalkozás által, a polgárok érdekeinek védelme mellett. A 2002/21/EK irányelv előírja a tagállamok számára a nyilvános hírközlő hálózatok integritásának és biztonságának fenntartását, továbbá olyan kötelezettségeket fogalmaz meg, miszerint a nyilvános hírközlő hálózatokat szolgáltató és a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó vállalkozásoknak műszaki és szervezési intézkedéseket kell tenniük a hálózatok és szolgáltatások biztonságát fenyegető kockázatok megfelelő kezelése érdekében. Az irányelv az ilyen kötelezettségek teljesítésének biztosítása érdekében a nemzeti szabályozó hatóságok hatásköréről is rendelkezik, beleértve a kötelező erejű utasítások kiadására vonatkozó hatáskört is.

(12) Ezen túlmenően a 2002/20/EK európai parlamenti és tanácsi irányelv ([8]) lehetővé teszi a tagállamok számára, hogy a jogosulatlan hozzáférés elleni, a nyilvános hálózatok biztonságára vonatkozó feltételeket csatoljanak az általános felhatalmazáshoz, a közlések titkosságának a 2002/58/EK európai parlamenti és tanácsi irányelv ([9]) szerinti védelme céljából.

(13) E kötelezettségek végrehajtásának támogatása érdekében az Unió számos együttműködési testületet hozott létre. Az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA), a Bizottság, a tagállamok és a nemzeti szabályozó hatóságok technikai iránymutatásokat dolgoztak ki a nemzeti szabályozó hatóságok számára a biztonsági események bejelentésére, a biztonsági intézkedésekre, valamint a fenyegetésekre és eszközökre vonatkozóan ([10]). Az (EU) 2016/1148 európai parlamenti és tanácsi irányelv ([11]) által létrehozott együttműködési csoport (a továbbiakban: az együttműködési csoport) az illetékes hatóságokat tömöríti az együttműködés támogatása és megkönnyítése érdekében, különösen azáltal, hogy stratégiai iránymutatást nyújt a számítógép-biztonsági eseményekre reagáló csoportok hálózatának tevékenységeihez, amely technikai szinten elősegíti az operatív együttműködést.

(14) A jövőbeli európai kiberbiztonsági tanúsítási rendszernek ([12]) fontos támogató eszközként kell szolgálnia a biztonság egységes szintjének előmozdításához. Lehetővé kell tennie kiberbiztonsági tanúsítási rendszerek kidolgozását annak érdekében, hogy kielégítse az 5G-hez kapcsolódó felszerelések és szoftverek felhasználóinak igényeit. Ezeknek az infrastruktúráknak a kritikus jelentőségére tekintettel az 5G hálózatokhoz használt információs és kommunikációs technológiai termékekre, szolgáltatásokra és eljárásokra vonatkozó európai kiberbiztonsági tanúsítási rendszerek fejlesztésének azonnali prioritást kell képeznie. A tagállamoknak és a piaci szereplőknek aktívan részt kell venniük az ilyen tanúsítási rendszerek kidolgozásában, beleértve az 5G hálózatok egyedi védelmi profiljának meghatározásához nyújtott támogatást.

(15) Harmonizált uniós jogszabályok hiányában a tagállamok az uniós joggal összhangban elfogadott nemzeti műszaki előírások útján elrendelhetik valamely európai kiberbiztonsági tanúsítási rendszer kötelező jellegét. A tagállamok a közbeszerzések és a 2014/24/EU európai parlamenti és tanácsi irányelv ([13]) kontextusában hozzáférnek európai kiberbiztonsági tanúsítási rendszerekhez, és támogathatnák segítségnyújtási mechanizmusok – például egy támogatási pont – kialakítását, amelyek kiberbiztonsági megoldások közszférába tartozó vásárlók általi beszerzését szolgálnák.

(16) Az adatok és a magánélet magas szintű védelme fontos eleme az 5G hálózatok biztonságának. Uniós szinten is meghatározták azokat a szabályokat, amelyek biztosítják a személyes adatok kezelésének biztonságát, többek között az elektronikus hírközlés során. Az általános adatvédelmi rendelet ([14]) előírja, hogy a személyes adatokat olyan módon kell kezelni, amely szavatolja azok biztonságát, beleértve a személyes adatokhoz vagy a kezelésükhöz használt felszereléshez való jogosulatlan hozzáféréssel, vagy az ilyen adatok vagy felszerelések

([6]) Az Európai Parlament és a Tanács 2002/21/EK irányelve (2002. március 7.) az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közös keretszabályozásáról (Keretirányelv) (HL L 108., 2002.4.24., 33. o.), valamint a külön irányelvek.

([7]) Az Európai Parlament és a Tanács (EU) 2018/1972 irányelve (2018. december 11.) az Európai Elektronikus Hírközlési Kódex létrehozásáról (HL L 321., 2018.12.17., 36. o.).

([8]) Az Európai Parlament és a Tanács 2002/20/EK irányelve (2002. március 7.) az elektronikus hírközlő hálózatok és az elektronikus hírközlési szolgáltatások engedélyezéséről (Engedélyezési irányelv) (HL L 108., 2002.4.24., 21. o.).

([9]) Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv) (HL L 201., 2002.7.31., 37. o.).

([10]) https://resilience.enisa.europa.eu/article-13.

([11]) Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (HL L 194., 2016.7.19., 1. o.).

([12]) Javaslat – Az Európai Parlament és a Tanács rendelete az ENISA-ról, az „Európai Uniós Kiberbiztonsági Ügynökségről”, az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról („kiberbiztonsági jogszabály”), COM(2017) 477 final – 2017/0225 (COD).

([13]) Az Európai Parlament és a Tanács 2014/24/EU irányelve (2014. február 26.) a közbeszerzésről és a 2004/18/EK irányelv hatályon kívül helyezéséről (HL L 94., 2014.3.28., 65. o.).

([14]) Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o.).

jogosulatlan használatával szembeni védelmet is. Az elektronikus hírközlési adatvédelmi irányelv külön szabályokat állapít meg a közlések titkosságának és a végfelhasználók végberendezéseinek védelmére. Emellett kötelezi a szolgáltatókat, hogy tegyenek megfelelő technikai és szervezési intézkedéseket szolgáltatásaik biztonságának védelme érdekében.

(17) Az Unió elfogadott egy olyan eszközt is, amely védeni fogja a kritikus infrastruktúrákat és a technológiákat (például a kommunikáció során használtakat) azáltal, hogy lehetővé teszi a tagállamok számára a közvetlen külföldi befektetések biztonsági vagy közrendi okokból történő átvilágítását, és olyan együttműködési mechanizmust hoz létre, amelyben a tagállamok és a Bizottság információcserét folytathatnak és konkrét befektetésekkel kapcsolatos aggályokat vethetnek fel ([15]).

(18) A tagállamok és a piaci szereplők jelenleg fontos előkészítő lépéseket tesznek az 5G hálózatok széles körű bevezetésének lehetővé tétele érdekében. Több tagállam aggodalmát fejezte ki az 5G hálózatokkal kapcsolatos potenciális biztonsági kockázatokkal kapcsolatban az 5G hálózatok számára kijelölt rádiófrekvencia-sávokban történő használati jogok odaítélésére vonatkozó eljárások végrehajtása keretében ([16]), és vizsgálták az e kockázatok kezelésére szolgáló lehetséges intézkedéseket.

(19) Az 5G hálózatokon belüli kiberbiztonsági kockázatok kezelése során figyelembe kell venni mind a technikai, mind az egyéb tényezőket. A technikai tényezők közé tartozhatnak az olyan kiberbiztonsági sebezhetőségek, amelyek az információkhoz való jogosulatlan hozzáférésre (kiberkémkedés akár gazdasági, akár politikai okokból) vagy más rosszhiszemű célra is felhasználhatók (a rendszerek és adatok megzavarását vagy megsemmisítését célzó kibertámadások). A figyelembe veendő szempontok a hálózatok védelmének szükségessége teljes életciklusuk során, valamint az, hogy a védelemnek minden érintett berendezésre ki kell terjednie, az 5G hálózatok tervezési, fejlesztési, közbeszerzési, kiépítési, üzemeltetési és fenntartási szakaszai során is.

(20) Egyéb tényezők lehetnek az információs és kommunikációs technológiai berendezések beszállítóira vonatkozó szabályozási vagy egyéb követelmények. Az ilyen tényezők jelentőségének értékelésénél figyelembe kell venni többek között a harmadik ország által gyakorolt befolyás általános kockázatát, különösen az irányítási modell, a biztonságra vonatkozó együttműködési megállapodások hiánya vagy az Unió és az érintett harmadik ország közötti hasonló adatvédelmi megállapodások – például megfelelőségi határozatok – tekintetében, illetve azt, hogy ez az ország részese-e a kiberbiztonsággal, a kiberbűnözés elleni küzdelemmel vagy az adatvédelemmel kapcsolatos többoldalú, nemzetközi vagy kétoldalú megállapodásoknak.

(21) Az 5G hálózatok kiberbiztonságára vonatkozó uniós megközelítés kidolgozásának fontos lépéseként a kockázatértékelést tagállami szinten kell elvégezni és lezárni. Ez segítené a tagállamokat a biztonsági követelményekre és a kockázatkezelésre vonatkozó tagállami intézkedések ezen értékelés szerint történő kiigazításában.

(22) Az ilyen kiberbiztonsági fenyegetések kezelését célzó intézkedések hatékonyságának biztosítása érdekében olyan koordinációs intézkedéseket kell kidolgozni, amelyek elengedhetetlenek a belső piac zavartalan működéséhez, valamint a személyes adatok és a magánélet védelméhez.

(23) A nemzeti kockázatértékeléseknek kell az összehangolt uniós kockázatértékelés alapjául szolgálniuk, amely a veszélyek feltérképezéséből és egy közös felülvizsgálatból áll, ezt a tagállamok a Bizottság támogatásával és az Európai Uniós Kiberbiztonsági Ügynökséggel (ENISA) közösen végzik el.

(24) A nemzeti és uniós kockázatértékeléseket figyelembe véve az együttműködési csoportnak meg kell határoznia a kiberbiztonsági kockázatok típusainak azonosítására szolgáló eszköztárat, valamint az olyan területek kockázatainak csökkentésére irányuló lehetséges intézkedéseket, mint a tanúsítás, a tesztelés és a hozzáférés-ellenőrzés. A csoportnak ezenkívül meg kell határoznia az egy vagy több tagállam által azonosított kockázatok kezelésére alkalmas lehetséges egyedi intézkedéseket. Az együttműködési csoportnak az Európai Uniós Kiberbiztonsági Ügynökség (ENISA), az Europol, az Európai Elektronikus Hírközlési Szabályozók Testülete (BEREC) és az Európai Unió Helyzetelemző Központjának támogatására kell támaszkodnia. Ez az eszköztár arra szolgál, hogy tanácsokkal lássa el a Bizottságot a minimális közös követelmények kidolgozásával kapcsolatban, amelyekre az 5G hálózatok magas szintű, az Unió egész területén érvényesülő kiberbiztonságának további biztosítása érdekében van szükség.

(25) Amennyiben intézkedéseket hoznak a kiberbiztonsági kockázatok kezelésére, egy hálózat kiépítésekor figyelembe kell venni, hogy a kiberbiztonság előmozdítását sokféle beszállítón keresztül kell megvalósítani.

([15]) Az Európai Parlament és a Tanács (EU) 2019/452 rendelete (2019. március 19.) az Unióba irányuló közvetlen külföldi befektetések átvilágítási keretének létrehozásáról (HL L 79. I, 2019.3.21., 1. o.).

([16]) 2019-re 11 tagállamban van legalább egy spektrumsávban aukciós eljárás ütemezve, ezek: Ausztria, Belgium, Csehország, Franciaország, Németország, Görögország, Magyarország, Írország, Hollandia, Litvánia, Portugália. 2020-ban további hat árverés várható: Spanyolországban, Máltán, Litvániában (eltérő frekvenciák), Szlovákiában, Lengyelországban és az Egyesült Királyságban. *Forrás:* http://5gobservatory.eu/observatory-overview/observatory-reports/.

(26) Ez az ajánlás nem sértheti a tagállamoknak a közbiztonsággal, a védelemmel és a nemzetbiztonsággal kapcsolatos tevékenységeire, illetve az államnak a büntetőjog területén végzett tevékenységeire vonatkozó hatáskörét, beleértve a tagállamok azon jogát, hogy piacaikról nemzetbiztonsági okokból szolgáltatókat vagy beszállítókat zárjanak ki.

ELFOGADTA EZT AZ AJÁNLÁST:

I. **CÉLKITŰZÉSEK**

(1) Az 5G hálózatok kiberbiztonságát biztosító uniós megközelítés kidolgozásának támogatása érdekében ez az ajánlás meghatározza azokat az intézkedéseket, amelyeket meg kell hozni annak érdekében, hogy:

a) a tagállamok fel tudják mérni az 5G hálózatokat nemzeti szinten érintő kiberbiztonsági kockázatokat, és meg tudják tenni a szükséges biztonsági intézkedéseket;

b) a tagállamok és az érintett uniós intézmények, ügynökségek és egyéb szervek közösen dolgozzanak ki egy nemzeti kockázatértékelésre épülő, összehangolt uniós kockázatértékelést;

c) az (EU) 2016/1148 irányelv alapján létrehozott együttműködési csoport (együttműködési csoport) meghatározza a digitális ökoszisztémát, különösen az 5G hálózatokat kiszolgáló infrastruktúrákkal kapcsolatos kiberbiztonsági kockázatokat csökkentő lehetséges közös intézkedéseket.

II. **FOGALOMMEGHATÁROZÁSOK**

(2) Ezen ajánlás alkalmazásában:

a) „5 G hálózatok”: a mobil és vezeték nélküli kommunikációs technológiákkal kapcsolatos releváns hálózati infrastrukturális elemek összessége, amelyeket olyan kiváló teljesítményjellemzőkkel rendelkező konnektivitási szolgáltatásokban és hozzáadott értéket képviselő szolgáltatásokban alkalmaznak, mint a nagyon nagy adatátviteli sebesség és kapacitás, az alacsony válaszidő, a nagy fokú megbízhatóság vagy az összekapcsolt eszközök nagy számának támogatása. Ezek magukban foglalhatnak meglévő hálózati elemeket is, amelyek a mobil és vezeték nélküli kommunikációs technológiák korábbi generációin alapulnak, mint például a 4G vagy a 3G. Az 5G hálózatokat úgy kell értelmezni, hogy azok a hálózat valamennyi releváns részét magukban foglalják.

b) „a digitális ökoszisztémát kiszolgáló infrastruktúra”: a gazdaság és a társadalomtudomány területén használt kritikus alkalmazások széles körénél a digitalizálást lehetővé tevő infrastruktúra.

III. **TAGÁLLAMI SZINTŰ FELLÉPÉS**

(3) A tagállamoknak 2019. június 30-ig el kell végezniük az 5G hálózati infrastruktúra kockázatértékelését, beleértve a legérzékenyebb elemek azonosítását, amelyek esetében a biztonság megsértésének jelentős negatív hatása lenne. Ugyanezen időpontig a tagállamoknak felül kell vizsgálniuk a nemzeti szinten alkalmazandó biztonsági követelményeket és kockázatkezelési módszereket, hogy figyelembe vegyék azokat a kiberbiztonsági fenyegetéseket, amelyeket i. a technikai tényezők, például az 5G hálózatok egyedi műszaki jellemzői, valamint ii. egyéb olyan tényezők, mint az információs és kommunikációs technológiai berendezések beszállítóira harmadik országokban esetlegesen alkalmazandó jogi és szakpolitikai keretek jelentenek.

(4) E nemzeti kockázatértékelés és felülvizsgálat alapján, valamint figyelembe véve az uniós szinten folyamatban lévő összehangolt fellépést, a tagállamoknak az alábbiakat kell tenniük:

a) frissíteniük kell az 5G hálózatok tekintetében alkalmazott biztonsági követelményeket és kockázatkezelési módszereket;

b) aktualizálniuk kell a nyilvános hírközlő hálózatokat szolgáltató vagy nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó vállalkozások számára a 2002/21/EK irányelv 13. cikkének a) és b) pontja értelmében előírt kötelezettségeket;

c) feltételekkel kell bővíteniük a nyilvános hálózatok jogosulatlan hozzáféréssel szembeni biztonságával kapcsolatos általános engedélyezést, és kötelezettségvállalást kell kérniük a következő eljárásokban részt vevő vállalkozások részéről arra vonatkozóan, hogy a 2002/20/EK irányelvnek megfelelően az 5G sávokban adják meg a rádiófrekvencia-használati jogokat a hálózatokra vonatkozó biztonsági követelmények betartása tekintetében.

d) egyéb megelőző intézkedéseket kell alkalmazniuk a lehetséges kiberbiztonsági kockázatok csökkentése érdekében.

(5) A negyedik pontban említett intézkedéseknek magukban kell foglalniuk a beszállítók és az üzemeltetők megerősített kötelezettségét arra vonatkozóan, hogy biztosítsák a hálózatok érzékeny részeinek biztonságát, illetve adott esetben az illetékes nemzeti hatóságok számára megfelelő tájékoztatást nyújtsanak az elektronikus hírközlő hálózatok tervezett változásaival kapcsolatban, ezenkívül az intézkedéseknek követelményeket kell tartalmazniuk a nemzeti ellenőrző/tanúsító laboratóriumok biztonsági és integritási célokból előzetesen tesztelt, meghatározott információtechnológiai összetevőire és rendszereire vonatkozóan.

(6) A közös biztonsági felülvizsgálatokat két vagy több tagállamnak kell elvégeznie – felhasználva és megosztva a megfelelő műszaki szakértelmet és létesítményeket a digitális ökoszisztémát és az 5G hálózatokat kiszolgáló infrastruktúrákkal kapcsolatban – például abban az esetben, ha ugyanaz a vállalkozás egynél több tagállamban is üzemeltet vagy épít hálózati infrastruktúrát, vagy ha a hálózati konfigurációk jelentős hasonlóságokat mutatnak. Az Európai Uniós Kiberbiztonsági Ügynökségnek (ENISA), az Europolnak és az Európai Elektronikus Hírközlési Szabályozók Testületének (BEREC) prioritásként kell kezelni a tagállamok támogatását ezen a területen. A felülvizsgálatok eredményeit továbbítani kell az együttműködési csoportnak és a számítógép-biztonsági eseményekre reagáló csoportok hálózatának.

IV. UNIÓS SZINTŰ ÖSSZEHANGOLT FELLÉPÉS

(7) Annak érdekében, hogy közös megközelítést dolgozzanak ki az 5G hálózatok kapcsán felmerülő kiberbiztonsági kockázatok kezelésére, a tagállamoknak 2019. április 30-ig el kell indítaniuk egy célzott munkafolyamatot az együttműködési csoportban. A tagállamoknak fel kell kérniük az érintett hatóságokat, hogy adott esetben vegyenek részt az együttműködési csoport munkájában.

Összehangolt európai kockázatértékelés

(8) A tagállamoknak információcserét kell folytatniuk egymással és az érintett uniós szervekkel annak érdekében, hogy felhívják a figyelmet az 5G hálózatokkal kapcsolatos meglévő és lehetséges kiberbiztonsági kockázatokra.

(9) A tagállamoknak 2019. július 15-ig továbbítaniuk kell nemzeti kockázatértékeléseiket a Bizottságnak és az Európai Uniós Kiberbiztonsági Ügynökségnek (ENISA).

(10) Az Európai Uniós Kiberbiztonsági Ügynökségnek (ENISA) fel kell térképeznie az 5G hálózatok által jelentett fenyegetéseket. Az együttműködési csoportnak és az (EU) 2016/1148 irányelv értelmében létrehozott, számítógép-biztonsági eseményekre reagáló csoportoknak támogatnia kell ezt a folyamatot.

(11) Mindezen elemeket figyelembe véve a tagállamoknak – a Bizottság támogatásával és az Európai Uniós Kiberbiztonsági Ügynökséggel (ENISA) együtt – 2019. október 1-jéig el kell végezniük a digitális ökoszisztémát, különösen az 5G hálózatokat kiszolgáló infrastruktúrákkal kapcsolatos kockázatoknak való uniós szintű kitettség közös felülvizsgálatát.

(12) E közös felülvizsgálat során prioritásként kell kezelni az 5G hálózatok alapelemeihez kapcsolódó különösen érzékeny vagy sérülékeny elemekre vonatkozó kockázatok, illetve a műveleti és karbantartási központtal, valamint az ipari alkalmazásokhoz használt 5G hozzáférési hálózati elemekkel kapcsolatos kockázatok elemzését.

(13) A második szakaszban ezt a közös felülvizsgálatot ki kell terjeszteni a digitális értéklánc más stratégiai elemeire is.

A kockázatok kezelésére szolgáló közös uniós eszköztár

(14) Az együttműködési csoport munkája során meg kell határozni a 4. pontban előirányzott, tagállami szinten alkalmazott bevált módszereket. A bevált nemzeti módszerek alapján 2019. december 31-ig meg kell állapodni a nemzeti és uniós szinten azonosított kiberbiztonsági kockázatok csökkentését célzó megfelelő, hatékony és arányos kockázatkezelési intézkedések eszköztárában, amely a Bizottság számára tanácsadást biztosítana az 5G hálózatok magas szintű kiberbiztonságának az egész Unióban történő további biztosítása érdekében szükséges minimális közös követelmények kidolgozására vonatkozóan.

(15) Ennek az eszköztárnak a következőket kell tartalmaznia:

a) az 5G hálózatok kiberbiztonságát érintő biztonsági kockázatok típusainak jegyzéke (például az ellátási láncra vonatkozó kockázat, a szoftverek sebezhetőségi kockázata, a hozzáférés-ellenőrzés kockázata, az információs és kommunikációs technológiai berendezések beszállítóira harmadik országokban esetlegesen alkalmazandó jogi és szakpolitikai keretből eredő kockázatok); valamint

b) lehetséges kockázatcsökkentő intézkedések (pl. harmadik fél általi tanúsítás hardver, szoftver vagy szolgáltatások esetében, hivatalos hardver- és szoftvertesztek vagy megfelelőségi ellenőrzések, a hozzáférés ellenőrzését és végrehajtását biztosító folyamatok, azon termékek, szolgáltatások vagy beszállítók azonosítása, amelyeket potenciálisan nem tekintenek biztonságosnak stb.). Ezeknek az intézkedéseknek a kockázatértékelést követően egy vagy több tagállamban azonosított valamennyi típusú biztonsági kockázatra kell kiterjedniük.

(16) Az 5G hálózatok tekintetében releváns európai kiberbiztonsági tanúsítási rendszerek kidolgozása után a tagállamoknak az uniós joggal összhangban el kell fogadniuk a nemzeti műszaki előírásokat, amelyek előírják az e rendszerek hatálya alá tartozó információs és kommunikációs technológiai termékek, szolgáltatások vagy rendszerek kötelező tanúsítását.

(17) A tagállamoknak a Bizottsággal együtt meg kell határozniuk a nyilvános hálózatok jogosulatlan hozzáféréssel szembeni biztonságával kapcsolatos feltételeket, amelyekkel ki kell egészíteniük az általános engedélyezést és a hálózatokra vonatkozó biztonsági követelményeket abból a célból, hogy kötelezettségvállalást kérjenek a vállalkozásoktól, amelyek részt vesznek az 5G sávok spektrumhasználati jogának a 2002/20/EK irányelv szerinti biztosításával kapcsolatos eljárásokban. Ezeket – amennyiben lehetséges – a (4) bekezdés c) pontjában említett intézkedéseknek kell tükrözniük.

(18) A tagállamoknak együtt kell működniük a Bizottsággal olyan konkrét biztonsági követelmények kidolgozása érdekében, amelyeket az 5G hálózatokkal kapcsolatos közbeszerzések keretében alkalmazni lehet. Ennek magában kell foglalnia a kiberbiztonsági tanúsítási rendszerek közbeszerzési eljárásokban való végrehajtására vonatkozó kötelező követelményeket, amennyiben ezek a rendszerek még nem kötelezőek minden beszállítóra és üzemeltetőre nézve.

V. **FELÜLVIZSGÁLAT**

(19) A tagállamoknak együtt kell működniük a Bizottsággal ezen ajánlás hatásainak 2020. október 1-jéig történő értékelése érdekében, a megfelelő további lépések meghatározása céljából. Az értékelésnek figyelembe kell vennie az összehangolt uniós kockázatértékelés eredményét és az uniós eszköztárat.

Kelt Strasbourgban, 2019. március 26-án.

a Bizottság részéről

Julian KING

a Bizottság tagja