2026/589

2026.3.16.

A TANÁCS (EU) 2026/589 VÉGREHAJTÁSI RENDELETE

(2026. március 16.)

az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről szóló (EU) 2019/796 rendelet végrehajtásáról

AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről szóló, 2019. május 17-i (EU) 2019/796 tanácsi rendeletre [1] és különösen annak 13. cikke (1) bekezdésére,

tekintettel az Unió külügyi és biztonságpolitikai főképviselőjének javaslatára,

mivel:

(1) A Tanács 2019. május 17-én elfogadta az (EU) 2019/796 rendeletet.

(2) A tartós kiberfenyegetés mögött álló szereplőkkel szembeni lankadatlan, személyre szabott és koordinált uniós fellépés részeként két természetes személyt és három szervezetet fel kell venni a korlátozó intézkedések hatálya alá tartozó természetes és jogi személyeknek, szervezeteknek és szerveknek az (EU) 2019/796 rendelet I. mellékletében foglalt jegyzékébe. Az említett természetes személyek és szervezetek felelősek olyan jelentős hatású kibertámadásokért, amelyek az Unióra vagy a tagállamaira nézve külső fenyegetést jelentenek, vagy részt vesznek azokban.

(3) Az (EU) 2019/796 rendelet I. mellékletét ezért ennek megfelelően módosítani kell,

ELFOGADTA EZT A RENDELETET:

1. cikk

Az (EU) 2019/796 rendelet I. melléklete e rendelet mellékletének megfelelően módosul.

2. cikk

Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetésének napján lép hatályba.

Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

Kelt Brüsszelben, 2026. március 16-án.

a Tanács részéről

az elnök

K. KALLAS

[1] HL L 129. I., 2019.5.17., 1. o., ELI: http://data.europa.eu/eli/reg/2019/796/oj.

MELLÉKLET

Az (EU) 2019/796 rendelet I. melléklete a következőképpen módosul:

1. Az „A. Természetes személyek” cím alatt a szöveg a következő bejegyzésekkel egészül ki:

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
„18.	CHEN Cheng	陈诚 (kínai írásmód szerint) más néven: Jesse Chen lengmo l3n6m0 Születési idő: 1984.10.20. Születési hely: Yancheng, Jiangsu, China Állampolgárság: kínai Nem: férfi	Chen Cheng kínai üzletember, az Anxun Information Technology Co. Ltd. társalapítója és egyik vezérigazgatója (műveleti igazgatója, Chief Operating Officer). Az említett vállalat szecsuáni fióktelepének az egyik jogi képviselője is. Az Anxun Information Technology Co. Ltd. – más néven i-Soon – a Kínai Népköztársaságban székhellyel rendelkező vállalat, amely »bérhacker« szolgáltatásokat kínál. Az Anxun Information Technology Co. Ltd. a tagállamok kritikus infrastruktúráját és kritikus állami funkcióit vette célba, valamint minősített adatokhoz fért hozzá, és ilyen adatokat értékesített. Továbbá, az Anxun Information Technology Co. Ltd. több harmadik állam kormányát is megtámadta, fenyegetve ezáltal az Uniónak az Európai Unióról szóló szerződés 21. cikke (2) bekezdésének a)–c) pontjában meghatározott közös kül- és biztonságpolitikai célkitűzéseit. Az Anxun Information Technology Co. Ltd. jelentős gazdasági hasznot húz a nyújtott szolgáltatásokból. Az Anxun Information Technology Co. Ltd.-t ezért felelősség terheli olyan jelentős hatású kibertámadásokért, amelyek külső fenyegetést jelentenek az Unióra és tagállamaira nézve, valamint harmadik államok elleni támadásokért. E kapacitásában Chen Chenget felelősség terheli olyan jelentős hatású kibertámadásokért, amelyek külső fenyegetést jelentenek a tagállamokra nézve, valamint harmadik államok elleni, jelentős hatású kibertámadásokért, és részt vesz azokban.	2026.3.16.

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
19.	WU Haibo	吴海波 (kínai írásmód szerint) más néven: shutdown shutd0wn Születési hely: China Állampolgárság: kínai Nem: férfi	Wu Haibo kínai üzletember, az Anxun Information Technology Ltd. társalapítója és egyik vezérigazgatója (Chief Executive Officer). Az Anxun Information Technology Co. Ltd. sanghaji fióktelepének (»anyavállalatiság«) jogi képviselője, elnöke és vezérigazgatója is. Továbbá, eljár az említett vállalat szecsuáni fióktelepének jogi képviselőjeként. Az Anxun Information Technology Co. Ltd. – más néven i-Soon – a Kínai Népköztársaságban székhellyel rendelkező vállalat, amely »bérhacker« szolgáltatásokat kínál. Az Anxun Information Technology Co. Ltd. a tagállamok kritikus infrastruktúráját és kritikus állami funkcióit vette célba, valamint minősített adatokhoz fért hozzá, és ilyen adatokat értékesített. Továbbá, az Anxun Information Technology Co. Ltd. több harmadik állam kormányát is megtámadta, fenyegetve ezáltal az Uniónak az Európai Unióról szóló szerződés 21. cikke (2) bekezdésének a)–c) pontjában meghatározott közös kül- és biztonságpolitikai célkitűzéseit. Az Anxun Information Technology Co. Ltd. jelentős gazdasági hasznot húz a nyújtott szolgáltatásokból. Az Anxun Information Technology Co. Ltd.-t ezért felelősség terheli olyan jelentős hatású kibertámadásokért, amelyek külső fenyegetést jelentenek a tagállamokra nézve, valamint harmadik államok elleni támadásokért. Wu Haibo részt vett a tagállamok ellen megkísérelt, jelentős hatású kibertámadások irányításában és ösztönzésében. E kapacitásában felelősség terheli olyan jelentős hatású kibertámadásokért, amelyek külső fenyegetést jelentenek a tagállamokra nézve, valamint harmadik államok elleni, jelentős hatású kibertámadásokért, és részt vesz azokban.	2026.3.16.”

2. A „B. Jogi személyek, szervezetek vagy szervek” cím alatt a szöveg a következő bejegyzésekkel egészül ki:

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
„5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (kínai írásmód szerint) más néven: Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited Cím: Fenghao East Road, Room 103, Building 6, No. 9, Beijing Haidian District, China A bejegyzés helye: Beijing, China A bejegyzés dátuma: 2010.9.2. Egységes társasági hitelazonosító: 91110108562135265P	Az Integration Technology Group a Kínai Népköztársaságban székhellyel rendelkező kiberbiztonsági vállalkozás, amely elősegítette a magas szintű állandó fenyegetést (APT) jelentő Flax Typhoonhoz kapcsolódó kibertámadásokat. Az említett APT az Integrity Technology Group termékeit és technológiáját használta a számítógépes hálózatok kihasználására irányuló tevékenységeinek végrehajtásához. Az Integrity Technology Group termékeit azóta a tagállamokban, valamint Európa-szerte és világszerte más országokban felhasználták a dolgok internetéhez (Internet of Things) tartozó eszközök kompromittálására és az azokhoz való hozzáférésre. 2022 és 2023 között a Flax Typhoon hat tagállamban legalább 65 600, a dolgok internetéhez tartozó eszközhöz fért hozzá az Integrity Technology Group termékeinek felhasználásával. Ennélfogva az Integrity Technology Group kereskedelmi termékeit és infrastruktúráját rutinszerűen használták a tagállamok és harmadik államok elleni kibertámadásokban. Következésképpen az Integrity Technology Group azáltal, hogy hatást gyakorol a digitális infrastruktúrával kapcsolatos információs rendszerekre, technikai és anyagi támogatást nyújt olyan jelentős hatású kibertámadásokhoz, amelyek külső fenyegetést jelentenek a tagállamokra és harmadik államokra nézve.	2026.3.16.

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
6.	Emennet Pasargad	más néven: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten A bejegyzés helye: Tehran, Iran Cégjegyzékszám: 554267 Az üzleti tevékenység fő helye: Tehran, Iran	Az Emennet Pasargad iráni kiberszereplő (vállalat), amely számos szervezetet vett célba, különösen a tagállamokban és az Egyesült Államokban (US). Az Emennet Pasargad – »Anzu Team« néven működve – a svédországi digitális infrastruktúrát vette célba, és kompromittálta a svéd SMS-szolgáltatást, ami számos embert érintett. Továbbá, a szervezet – »Holy Souls« néven eljárva – kompromittálta a Charlie Hebdo francia szatirikus folyóirat előfizetői adatbázisát, és azt a dark weben eladásra hirdette meg. Az Emennet Pasargad a párizsi olimpiai játékok során kompromittálta a hirdetőtáblákat, és dezinformációs kampányokat jelenített meg. Az Emennet Pasargad megkísérelt beavatkozni a 2020-as amerikai elnökválasztásokba is, veszélyeztetve a demokráciát és a jogállamiságot azáltal, hogy bizalmas információkat szerzett az egyesült államokbeli szavazókról, és jogtalan hozzáférést szerzett egy egyesült államokbeli médiavállalat számítógépes hálózatához. Az Emennet Pasargadot ezért felelősség terheli olyan jelentős hatású kibertámadásokért, amelyek külső fenyegetést jelentenek a tagállamokra nézve, valamint harmadik államok elleni, jelentős hatású kibertámadásokért.	2026.3.16.

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
7.	Anxun Information Technology Co. Ltd.	安洵信息技术有限公司 (kínai írásmód szerint) más néven: i-Soon Cím: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai Egységes társasági hitelazonosító: 91510105332025597A (szecsuáni fióktelep) Egységes társasági hitelazonosító: 91310116561906136G (sanghaji fióktelep) Honlap: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win Telefonszámok: +862161119992, +8605645893417, +8613761671735, +864000665915 E-mail-cím: shutdown@163.com, isoon2015@126.com, tao_tingting@i-soon.net, li_ping@i-soon.net	Az Anxun Information Technology Co. Ltd. a Kínai Népköztársaságban székhellyel rendelkező vállalat, amely »bérhacker« szolgáltatásokat kínál. A tagállamok kritikus infrastruktúráját és kritikus állami funkcióit vette célba, valamint minősített adatokhoz fért hozzá, és ilyen adatokat értékesített. Továbbá, az Anxun Information Technology Co. Ltd. több harmadik állam kormányát is megtámadta, fenyegetve ezáltal az Uniónak az Európai Unióról szóló szerződés 21. cikke (2) bekezdésének a)–c) pontjában meghatározott közös kül- és biztonságpolitikai célkitűzéseit. Az Anxun Information Technology Co. Ltd. jelentős gazdasági hasznot húz a nyújtott szolgáltatásokból. Az Anxun Information Technology Co. Ltd.-t ezért felelősség terheli olyan jelentős hatású kibertámadásokért, amelyek külső fenyegetést jelentenek a tagállamokra nézve, valamint harmadik államok elleni, jelentős hatású kibertámadásokért.	2026.3.16.”

ELI: http://data.europa.eu/eli/reg_impl/2026/589/oj