2026/589

16.3.2026

VYKONÁVACIE NARIADENIE RADY (EÚ) 2026/589

zo 16. marca 2026,

ktorým sa vykonáva nariadenie (EÚ) 2019/796 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty

RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Rady (EÚ) 2019/796 zo 17. mája 2019 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty ([1]), a najmä na jeho článok 13 ods. 1,

so zreteľom na návrh vysokej predstaviteľky Únie pre zahraničné veci a bezpečnostnú politiku,

keďže:

(1) Rada 17. mája 2019 prijala nariadenie (EÚ) 2019/796.

(2) V rámci trvalých, prispôsobených a koordinovaných opatrení Únie proti pretrvávajúcim aktérom v oblasti kybernetických hrozieb by sa do zoznamu fyzických a právnických osôb, subjektov a orgánov, na ktoré sa vzťahujú reštriktívne opatrenia, uvedeného v prílohe I k nariadeniu (EÚ) 2019/796 mali zaradiť dve fyzické osoby a tri subjekty. Uvedené fyzické osoby a subjekty sú zodpovedné za kybernetické útoky so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty, alebo sa na nich podieľajú.

(3) Príloha I k nariadeniu (EÚ) 2019/796 by sa preto mala zodpovedajúcim spôsobom zmeniť,

PRIJALA TOTO NARIADENIE:

Článok 1

Príloha I k nariadeniu (EÚ) 2019/796 sa mení v súlade s prílohou k tomuto nariadeniu.

Článok 2

Toto nariadenie nadobúda účinnosť dňom jeho uverejnenia v *Úradnom vestníku Európskej únie*.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 16. marca 2026

Za Radu
predsedníčka
K. KALLAS

([1]) Ú. v. EÚ L 129 I, 17.5.2019, s. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj.

PRÍLOHA

Príloha I k nariadeniu (EÚ) 2019/796 sa mení takto:

1. Do oddielu „A. Fyzické osoby“ sa dopĺňajú tieto záznamy:

	Meno	Identifikačné údaje	Odôvodnenie	Dátum zaradenia na zoznam
„18.	CHEN Cheng	陈诚 (v čínštine) alias: Jesse Chen lengmo l3n6m0 Dátum narodenia: 20.10.1984 Miesto narodenia: Yancheng, Jiangsu, Čína Štátna príslušnosť: čínska Pohlavie: muž	Chen Cheng je čínsky podnikateľ, spoluzakladateľ a jeden z generálnych riaditeľov (prevádzkový riaditeľ) spoločnosti Anxun Information Technology Co. Ltd. Je tiež právnym zástupcom pobočky uvedenej spoločnosti v Sečuane. Spoločnosť Anxun Information Technology Co. Ltd., známa aj ako i-Soon, je spoločnosť so sídlom v Čínskej ľudovej republike (ČĽR), ktorá ponúka služby ‚hackerstva na prenájom‘. Spoločnosť Anxun Information Technology Co. Ltd. sa zameriava na kritickú infraštruktúru a kritické štátne funkcie členských štátov, v minulosti získala prístup k utajovaným skutočnostiam a predala ich. Okrem toho spoločnosť Anxun Information Technology Co. Ltd. zaútočila na vlády rôznych tretích štátov, čím predstavuje hrozbu pre ciele spoločnej zahraničnej a bezpečnostnej politiky (SZBP) Únie, ako sú stanovené v článku 21 ods. 2 písm. a) až c) Zmluvy o Európskej únii. Spoločnosť Anxun Information Technology Co. Ltd. získava z poskytovaných služieb významný hospodársky prospech. Spoločnosť Anxun Information Technology Co. Ltd. je teda zodpovedná za kybernetické útoky so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu a jej členské štáty, ako aj útoky proti tretím štátom. Chen Cheng je vo svojej funkcii zodpovedný za kybernetické útoky so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre členské štáty, ako aj za kybernetické útoky so závažným vplyvom na tretie štáty, a je do týchto útokov zapojený.	16.3.2026

	Meno	Identifikačné údaje	Odôvodnenie	Dátum zaradenia na zoznam
19.	WU Haibo	吴海波 (v čínštine) alias: shutdown shutd0wn Miesto narodenia: Čína Štátna príslušnosť: čínska Pohlavie: muž	Wu Haibo je čínsky podnikateľ, spoluzakladateľ a jeden z generálnych riaditeľov (výkonný riaditeľ) spoločnosti Anxun Information Technology Co. Ltd. Je tiež právnym zástupcom, predsedom predstavenstva a generálnym riaditeľom tzv. materskej pobočky spoločnosti Anxun Information Technology Co. Ltd. v Šanghaji. Okrem toho vystupuje aj ako právny zástupca pobočky uvedenej spoločnosti v Sečuane. Spoločnosť Anxun Information Technology Co. Ltd., známa aj ako i-Soon, je spoločnosť so sídlom v Čínskej ľudovej republike (ČĽR), ktorá ponúka služby ‚hackerstva na prenájom'. Spoločnosť Anxun Information Technology Co. Ltd. sa zameriava na kritickú infraštruktúru a kritické štátne funkcie členských štátov, v minulosti získala prístup k utajovaným skutočnostiam a predala ich. Okrem toho spoločnosť Anxun Information Technology Co. Ltd. zaútočila na vlády rôznych tretích štátov, čím predstavuje hrozbu pre ciele spoločnej zahraničnej a bezpečnostnej politiky (SZBP) Únie, ako sú stanovené v článku 21 ods. 2 písm. a) až c) Zmluvy o Európskej únii. Spoločnosť Anxun Information Technology Co. Ltd. získava z poskytovaných služieb významný hospodársky prospech. Spoločnosť Anxun Information Technology Co. Ltd. je teda zodpovedná za kybernetické útoky so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre členské štáty, ako aj útoky proti tretím štátom. Wu Haibo sa podieľal na riadení a podpore pokusov o kybernetické útoky so závažným vplyvom na členské štáty. Vo svojej funkcii je zodpovedný za kybernetické útoky so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre členské štáty, ako aj za kybernetické útoky so závažným vplyvom na tretie štáty, a je do týchto útokov zapojený.	16.3.2026“.

2. Do oddielu „B. Právnické osoby, subjekty a orgány“ sa dopĺňajú tieto záznamy:

	Meno	Identifikačné údaje	Odôvodnenie	Dátum zaradenia na zoznam
„5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (v čínštine) alias: Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited Adresa: Fenghao East Road, Room 103, Building 6, No. 9, Beijing Haidian District, China Miesto registrácie: Peking, Čína Dátum registrácie: 2.9.2010 Kód jednotného sociálneho kreditu: 91110108562135265P	Integrity Technology Group je podnik pôsobiaci v oblasti kybernetickej bezpečnosti so sídlom v Čínskej ľudovej republike (ČĽR), ktorý uľahčil kybernetické útoky spojené so skupinou Flax Typhoon, ktorá predstavuje pokročilú pretrvávajúcu hrozbu (APT). Uvedená skupina využila produkty a technológie podniku Integrity Technology Group na realizáciu svojich činností využívania počítačovej siete. Produkty podniku Integrity Technology Group sa odvtedy používajú na ohrozovanie zariadení internetu vecí v členských štátoch, ako aj v krajinách po celej Európe a na celom svete a na prístup k nim. V rokoch 2022 až 2023 získala skupina Flax Typhoon pomocou produktov podniku Integrity Technology Group prístup aspoň k 65 600 zariadeniam internetu vecí v šiestich členských štátoch. Komerčné produkty a infraštruktúra podniku Integrity Technology Group sa teda bežne používali pri kybernetických útokoch proti členským štátom, ako aj tretím štátom. Podnik Integrity Technology Group preto tým, že ovplyvňuje informačné systémy digitálnej infraštruktúry, poskytuje technickú a materiálnu podporu pre kybernetické útoky so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre členské štáty a tretie štáty.	16.3.2026

	Meno	Identifikačné údaje	Odôvodnenie	Dátum zaradenia na zoznam
6.	Emennet Pasargad	alias: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten Miesto registrácie: Teherán, Irán Registračné číslo: 554267 Hlavné miesto podnikateľskej činnosti: Teherán, Irán	Emennet Pasargad je iránsky kybernetický aktér (spoločnosť), ktorý sa zameriava na mnohé subjekty najmä v členských štátoch, ako aj v Spojených štátoch (USA). Emennet Pasargad pôsobiaci pod aliasom ‚Anzu Team' sa zameral na digitálnu infraštruktúru vo Švédsku a narušil švédsku službu SMS, čo ovplyvnilo veľký počet ľudí. Okrem toho tento subjekt pod aliasom ‚Holy Souls' narušil databázu predplatiteľov francúzskeho satirického časopisu Charlie Hebdo a ponúkal ju na predaj na dark webe. Počas olympijských hier v Paríži Emennet Pasargad narušil reklamné bilbordy a prezentoval dezinformačné kampane. Emennet Pasargad sa tiež pokúsil zasahovať do prezidentských volieb v USA v roku 2020, čím ohrozil demokraciu a právny štát, pričom získal dôverné informácie o voličoch v USA a neoprávnený prístup k počítačovej sieti istej americkej mediálnej spoločnosti. Emennet Pasargad je preto zodpovedný za kybernetické útoky so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre členské štáty, a za kybernetické útoky so závažným vplyvom na tretí štát.	16.3.2026

	Meno	Identifikačné údaje	Odôvodnenie	Dátum zaradenia na zoznam
7.	Anxun Information Technology Co. Ltd.	安洵信息技术有限公司 (v čínštine) alias: i-Soon Adresa: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai Kód jednotného sociálneho kreditu: 91510105332025597A (pobočka v Sičuane) Kód jednotného sociálneho kreditu: 91310116561906136G (pobočka v Šanghaji) Webové sídlo: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win Telefónne čísla: +862161119992, +8605645893417, +8613761671735, +864000665915 E-mail: shutdown@163.com, isoon2015@126.com, tao_tingting@i-soon.net, li_ping@i-soon.net	Anxun Information Technology Co. Ltd. je spoločnosť so sídlom v Čínskej ľudovej republike, ktorá ponúka služby ‚hackerstva na prenájom'. Zameriava sa na kritickú infraštruktúru a kritické štátne funkcie členských štátov, v minulosti získala prístup k utajovaným skutočnostiam a predala ich. Okrem toho spoločnosť Anxun Information Technology Co. Ltd. zaútočila na vlády rôznych tretích štátov, čím predstavuje hrozbu pre ciele spoločnej zahraničnej a bezpečnostnej politiky (SZBP) Únie, ako sú stanovené v článku 21 ods. 2 písm. a) až c) Zmluvy o Európskej únii. Spoločnosť Anxun Information Technology Co. Ltd. získava z poskytovaných služieb významný hospodársky prospech. Spoločnosť Anxun Information Technology Co. Ltd. je preto zodpovedná za kybernetické útoky so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre členské štáty, ako aj za kybernetické útoky so závažným vplyvom na tretie štáty.	16.3.2026".