2026/589

16.3.2026.

PROVEDBENA UREDBA VIJEĆA (EU) 2026/589

od 16. ožujka 2026.

o provedbi Uredbe (EU) 2019/796 o mjerama ograničavanja protiv kibernapada koji predstavljaju prijetnju Uniji ili njezinim državama članicama

VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu Vijeća (EU) 2019/796 od 17. svibnja 2019. o mjerama ograničavanja protiv kibernapada koji predstavljaju prijetnju Uniji ili njezinim državama članicama ([1]), a posebno njezin članak 13. stavak 1.,

uzimajući u obzir prijedlog Visokog predstavnika Unije za vanjske poslove i sigurnosnu politiku,

budući da:

(1) Vijeće je 17. svibnja 2019. donijelo Uredbu (EU) 2019/796.

(2) U okviru trajnog, prilagođenog i usklađenog djelovanja Unije protiv aktera koji predstavljaju stalnu kibernetičku prijetnju dvije fizičke osobe i tri subjekta trebalo bi uvrstiti na popis fizičkih i pravnih osoba, subjekata i tijela koji podliježu mjerama ograničavanja naveden u Prilogu I. Uredbi (EU) 2019/796. Te su fizičke osobe i subjekti odgovorni za kibernetičke napade sa znatnim učinkom koji predstavljaju vanjsku prijetnju Uniji ili njezinim državama članicama ili su u njih uključene.

(3) Prilog I. Uredbi (EU) 2019/796 trebalo bi stoga na odgovarajući način izmijeniti,

DONIJELO JE OVU UREDBU:

Članak 1.

Prilog I. Uredbi (EU) 2019/796 mijenja se u skladu s Prilogom ovoj Uredbi.

Članak 2.

Ova Uredba stupa na snagu na dan objave u *Službenom listu Europske unije*.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu 16. ožujka 2026.

Za Vijeće

Predsjednica

K. KALLAS

([1]) SL L 129 I, 17.5.2019., str. 1., ELI: http://data.europa.eu/eli/reg/2019/796/oj.

PRILOG

Prilog I. Uredbi (EU) 2019/796 mijenja se kako slijedi:

1. sljedeći unosi dodaju se pod naslovom „A. Fizičke osobe”:

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
„18.	CHEN Cheng	陈诚 (kineski način pisanja) također poznat kao: Jesse Chen lengmo l3n6m0 Datum rođenja: 20.10.1984. Mjesto rođenja: Yancheng, Jiangsu, China (Kina) Državljanstvo: kinesko Spol: muški	Chen Cheng kineski je poslovni čovjek, suosnivač i jedan od glavnih direktora (glavni voditelj poslovanja) društva Anxun Information Technology Co. Ltd. Također je pravni zastupnik sečuanske podružnice tog društva. Anxun Information Technology Co. Ltd., poznato i kao i-Soon, društvo je sa sjedištem u Narodnoj Republici Kini (NRK) koje nudi usluge ‚najma hakiranja'. Meta društva Anxun Information Technology Co. Ltd. bile su kritična infrastruktura i ključne državne funkcije država članica te je pristupilo klasificiranim podacima i prodavalo ih. Osim toga, društvo Anxun Information Technology Co. Ltd. napalo je vlade raznih trećih zemalja i time predstavlja prijetnju ciljevima zajedničke vanjske i sigurnosne politike (ZVSP) Unije, kako su utvrđeni u članku 21. stavku 2. točkama od (a) do (c) Ugovora o Europskoj uniji. Društvo Anxun Information Technology Co. Ltd. ostvaruje znatnu gospodarsku korist od usluga koje pruža. Društvo Anxun Information Technology Co. Ltd. stoga je odgovorno za kibernetičke napade sa znatnim učinkom koji predstavljaju vanjsku prijetnju Uniji i njezinim državama članicama kao i za napade na treće zemlje. Chen Cheng u tom je svojstvu odgovoran za kibernetičke napade sa znatnim učinkom koji predstavljaju vanjsku prijetnju državama članicama, kao i za kibernetičke napade sa znatnim učinkom protiv trećih zemalja, te je uključen u te kibernetičke napade.	16.3.2026.

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
19.	WU Haibo	吴海波 (kineski način pisanja) također poznat kao: shutdown shutd0wn Mjesto rođenja: China (Kina) Državljanstvo: kinesko Spol: muški	Wu Haibo kineski je poslovni čovjek, suosnivač i jedan od glavnih direktora (glavni izvršni direktor) društva Anxun Information Technology Co. Ltd. Ujedno je pravni zastupnik, predsjednik i glavni direktor šangajske podružnice (‚matično društvo') društva Anxun Information Technology Co. Ltd. Osim toga, djeluje kao pravni zastupnik sečuanske podružnice tog društva. Anxun Information Technology Co. Ltd., poznato i kao i-Soon, društvo je sa sjedištem u Narodnoj Republici Kini (NRK) koje nudi usluge ‚najma hakiranja'. Meta društva Anxun Information Technology Co. Ltd. bile su kritična infrastruktura i ključne državne funkcije država članica te je pristupilo klasificiranim podacima i prodavalo ih. Osim toga, društvo Anxun Information Technology Co. Ltd. napalo je vlade raznih trećih zemalja, i time predstavlja prijetnju ciljevima zajedničke vanjske i sigurnosne politike (ZVSP) Unije, kako su utvrđeni u članku 21. stavku 2. točkama od (a) do (c) Ugovora o Europskoj uniji. Društvo Anxun Information Technology Co. Ltd. ostvaruje znatnu gospodarsku korist od usluga koje pruža. Društvo Anxun Information Technology Co. Ltd. stoga je odgovorno za kibernetičke napade sa znatnim učinkom koji predstavljaju vanjsku prijetnju državama članicama kao i za napade na treće zemlje. Wu Haibo sudjelovao je u vođenju i poticanju pokušaja kibernetičkih napada sa znatnim učinkom protiv država članica. U tom je svojstvu odgovoran za kibernetičke napade sa znatnim učinkom koji predstavljaju vanjsku prijetnju državama članicama, kao i za kibernetičke napade sa znatnim učinkom protiv trećih zemalja, te je uključen u te kibernetičke napade.	16.3.2026.”

2. sljedeći unosi dodaju se pod naslovom „B. Pravne osobe, subjekti i tijela”:

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
„5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (kineski način pisanja) također poznato kao: 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 Mjesto registracije: Beijing (Peking), China (Kina) Datum registracije: 2.9.2010. Jedinstveni socijalni kreditni broj: 91110108562135265P	Integrity Technology Group poduzeće je za kibernetičku sigurnost sa sjedištem u Narodnoj Republici Kini (NRK) koje je olakšalo kibernetičke napade povezane s naprednom stalnom prijetnjom (APT) Flax Typhoon. Taj je APT upotrebljavao proizvode i tehnologiju društva Integrity Technology Group za provedbu aktivnosti iskorištavanja računalne mreže. Proizvodi društva Integrity Technology Group od tada se upotrebljavaju za ugrožavanje uređaja interneta stvari i pristup njima u državama članicama, kao i u zemljama diljem Europe i u cijelom svijetu. U razdoblju od 2022. do 2023. Flax Typhoon pristupili su najmanje 65 600 uređaja interneta stvari u šest država članica upotrebom proizvoda društva Integrity Technology Group. Stoga su se komercijalni proizvodi i infrastruktura društva Integrity Technology Group rutinski upotrebljavali u kibernetičkim napadima na države članice i treće zemlje. Društvo Integrity Technology Group stoga utjecanjem na informacijske sustave povezane s digitalnom infrastrukturom pruža tehničku i materijalnu potporu za kibernetičke napade sa znatnim učinkom koji predstavljaju vanjsku prijetnju državama članicama i trećim državama.	16.3.2026.

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
6.	Emennet Pasargad	također poznato kao: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten Mjesto registracije: Tehran (Teheran), Iran Registracijski broj: 554267 Glavno sjedište: Tehran (Teheran), Iran	Društvo Emennet Pasargad iranski je kibernetički akter (društvo) čija su meta bili brojni subjekti, posebno u državama članicama i Sjedinjenim Američkim Državama (SAD). Društvo Emennet Pasargad, koje djeluje pod pseudonimom ‚Anzu Team', bilo je usmjereno na digitalnu infrastrukturu u Švedskoj i ugrozilo je švedsku SMS uslugu, što je utjecalo na velik broj osoba. Osim toga, djelujući pod pseudonimom ‚Holy Souls', taj je subjekt ugrozio bazu podataka pretplatnika francuskog satiričkog časopisa Charlie Hebdo te ju je oglašavao za prodaju na tamnoj mreži. Društvo Emennet Pasargad ugrožavalo je reklamne panoe tijekom Olimpijskih igara u Parizu i prikazivalo kampanje dezinformiranja. Društvo Emennet Pasargad također je pokušalo utjecati na predsjedničke izbore u SAD-u 2020., čime je ugrozilo demokraciju i vladavinu prava, tako što je pribavljalo povjerljive informacije o biračima u SAD-u i neovlašteno pristupalo računalnoj mreži američke medijske kuće. Društvo Emennet Pasargad stoga je odgovorno za kibernetičke napade sa znatnim učinkom koji predstavljaju vanjsku prijetnju državama članicama i za kibernetičke napade sa znatnim učinkom protiv treće zemlje.	16.3.2026.

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
7.	Anxun Information Technology Co. Ltd.	安洵信息技术有限公司 (kineski način pisanja) također poznato kao: i-Soon Adresa: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai Jedinstveni socijalni kreditni broj: 91510105332025597A (sečuanska podružnica) Jedinstveni socijalni kreditni broj: 91310116561906136G (šangajska podružnica) Internetske stranice: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win Brojevi telefona: +862161119992, +8605645893417, +8613761671735, +864000665915 E-adrese: shutdown@163.com, isoon2015@126.com, tao_tingting@i-soon.net, li_ping@i-soon.net	Anxun Information Technology Co. Ltd. društvo je sa sjedištem u Narodnoj Republici Kini (NRK) koje nudi usluge ‚najma hakiranja'. Meta tog društva bile su kritična infrastruktura i ključne državne funkcije država članica te je pristupilo klasificiranim podacima i prodavalo ih. Osim toga, društvo Anxun Information Technology Co. Ltd. napalo je vlade raznih trećih zemalja, i time predstavlja prijetnju ciljevima zajedničke vanjske i sigurnosne politike (ZVSP) Unije, kako su utvrđeni u članku 21. stavku 2. točkama od (a) do (c) Ugovora o Europskoj uniji. Društvo Anxun Information Technology Co. Ltd. ostvaruje znatnu gospodarsku korist od usluga koje pruža. Društvo Anxun Information Technology Co. Ltd. stoga je odgovorno za kibernetičke napade sa znatnim učinkom koji predstavljaju vanjsku prijetnju državama članicama, kao i za kibernetičke napade sa znatnim učinkom protiv trećih zemalja.	16.3.2026.”

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