2026/588

16.3.2026.

PADOMES LĒMUMS (KĀDP) 2026/588

(2026. gada 16. marts),

ar ko groza Lēmumu (KĀDP) 2019/797 par ierobežojošiem pasākumiem pret kiberuzbrukumiem, kuri apdraud Savienību vai tās dalībvalstis

EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienību un jo īpaši tā 29. pantu,

ņemot vērā Savienības Augstās pārstāves ārlietās un drošības politikas jautājumos priekšlikumu,

tā kā:

(1) Padome 2019. gada 17. maijā pieņēma Lēmumu (KĀDP) 2019/797 ([1]).

(2) Kā daļu no noturīgas, pielāgotas un koordinētas Savienības darbības pret pastāvīgiem kiberdraudu aktoriem Lēmuma (KĀDP) 2019/797 pielikumā ietvertajā to fizisko un juridisko personu, vienību un struktūru sarakstā, kurām piemēro ierobežojošus pasākumus, būtu jāiekļauj divas fiziskas personas un trīs vienības. Minētās personas un vienības ir atbildīgas par kiberuzbrukumiem ar būtisku ietekmi, kuri ir ārējs apdraudējums Savienībai vai tās dalībvalstīm, vai ir iesaistītas tajos.

(3) Tādēļ Lēmums (KĀDP) 2019/797 būtu attiecīgi jāgroza,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

Lēmuma (KĀDP) 2019/797 pielikumu groza saskaņā ar šā lēmuma pielikumu.

2. pants

Šis lēmums stājas spēkā dienā, kad to publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

Briselē, 2026. gada 16. martā

Padomes vārdā –

priekšsēdētāja

K. KALLAS

([1]) Padomes Lēmums (KĀDP) 2019/797 (2019. gada 17. maijs) par ierobežojošiem pasākumiem pret kiberuzbrukumiem, kuri apdraud Savienību vai tās dalībvalstis (OV L 129 I, 17.5.2019., 13. lpp., ELI: http://data.europa.eu/eli/dec/2019/797/oj).

PIELIKUMS

Lēmuma (KĀDP) 2019/797 pielikumu groza šādi:

1) iedaļā “A. Fiziskas personas” pievieno šādus ierakstus:

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
“18.	CHEN Cheng	陈诚 (ķīniešu rakstībā) jeb: Jesse Chen lengmo l3n6m0 Dzimšanas datums: 20.10.1984. Dzimšanas vieta: *Yancheng, Jiangsu*, Ķīna Valstspiederība: Ķīna Dzimums: vīrietis	*Chen Cheng* ir Ķīnas uzņēmējs, *Anxun Information Technology Co. Ltd*. līdzdibinātājs un viens no ģenerāldirektoriem (rīkotājdirektors). Viņš ir arī minētā uzņēmuma *Sichuan* biroja juridiskais pārstāvis. *Anxun Information Technology Co. Ltd*. jeb *i-Soon* ir Ķīnas Tautas Republikā (ĶTR) bāzēts uzņēmums, kas piedāvā nolīgtas kiberuzlaušanas (“*hacking for-hire*”) pakalpojumus. *Anxun Information Technology Co. Ltd*. ir vērsies pret dalībvalstu kritisko infrastruktūru un kritiskajām valsts funkcijām un piekļuvis klasificētai informācijai un to pārdevis. Turklāt *Anxun Information Technology Co. Ltd*. ir uzbrucis dažādu trešo valstu valdībām, tādējādi apdraudot Savienības kopējās ārpolitikas un drošības politikas (KĀDP) mērķus, kas izklāstīti Līguma par Eiropas Savienību 21. panta 2. punkta a) līdz c) apakšpunktā. *Anxun Information Technology Co. Ltd*. gūst būtisku ekonomisku labumu no sniegtajiem pakalpojumiem. Tāpēc *Anxun Information Technology Co. Ltd*. ir atbildīgs par kiberuzbrukumiem ar būtisku ietekmi, kas rada ārēju apdraudējumu Savienībai un tās dalībvalstīm, kā arī par uzbrukumiem pret trešām valstīm. Tādējādi *Chen Cheng*, pildot savas pilnvaras, ir atbildīgs par kiberuzbrukumiem ar būtisku ietekmi, kas rada ārēju apdraudējumu dalībvalstīm, kā arī par kiberuzbrukumiem ar būtisku ietekmi pret trešām valstīm, un ir iesaistīts šādos uzbrukumos.	16.3.2026.

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
19.	WU Haibo	吴海波 (ķīniešu rakstībā) jeb: shutdown shutd0wn Dzimšanas vieta: Ķīna Valstspiederība: Ķīna Dzimums: vīrietis	*Wu Haibo* ir Ķīnas uzņēmējs, *Anxun Information Technology Ltd* līdzdibinātājs un viens no ģenerāldirektoriem (izpilddirektors). Viņš ir arī *Anxun Information Technology Co. Ltd. Shanghai* biroja ("centrālais birojs") juridiskais pārstāvis, priekšsēdētājs un ģenerāldirektors. Turklāt viņš darbojas arī kā minētā uzņēmuma *Sichuan* biroja juridiskais pārstāvis. *Anxun Information Technology Co. Ltd.* jeb *i-Soon* ir Ķīnas Tautas Republikā (ĶTR) bāzēts uzņēmums, kas piedāvā nolīgtas kiberuzlaušanas ("*hacking for-hire*") pakalpojumus. *Anxun Information Technology Co. Ltd.* ir vērsies pret dalībvalstu kritisko infrastruktūru un kritiskajām valsts funkcijām un piekļuvis klasificētai informācijai un to pārdevis. Turklāt *Anxun Information Technology Co. Ltd.* ir uzbrucis dažādu trešo valstu valdībām, tādējādi apdraudot Savienības kopējās ārpolitikas un drošības politikas (KĀDP) mērķus, kas izklāstīti Līguma par Eiropas Savienību 21. panta 2. punkta a) līdz c) apakšpunktā. *Anxun Information Technology Co. Ltd.* gūst būtisku ekonomisku labumu no sniegtajiem pakalpojumiem. Tāpēc *Anxun Information Technology Co. Ltd.* ir atbildīgs par kiberuzbrukumiem ar būtisku ietekmi, kas rada ārēju apdraudējumu dalībvalstīm, kā arī par uzbrukumiem pret trešām valstīm. *Wu Haibo* bija iesaistīts tādu kiberuzbrukumu mēģinājumu vadīšanā un veicināšanā, kuriem ir būtiska ietekme uz dalībvalstīm. Tādējādi viņš, pildot savas pilnvaras, ir atbildīgs par kiberuzbrukumiem ar būtisku ietekmi, kas rada ārēju apdraudējumu dalībvalstīm, kā arī par kiberuzbrukumiem ar būtisku ietekmi pret trešām valstīm, un ir iesaistīts šādos uzbrukumos.	16.3.2026."

2) iedaļā “B. Juridiskas personas, vienības un struktūras” pievieno šādus ierakstus:

	Nosaukums	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
“5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (ķīniešu rakstībā) jeb: Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited Adrese: *Fenghao East Road, Room 103, Building 6, No. 9, Beijing Haidian District*, Ķīna Reģistrācijas vieta: *Beijing*, Ķīna Reģistrācijas datums: 2.9.2010. Vienotais sociālā kredīta kods: 91110108562135265P	*Integrity Technology Group* ir Ķīnas Tautas Republikā (ĶTR) bāzēts kiberdrošības uzņēmums, kas atviegloja kiberuzbrukumus, kuri saistīti ar *Advanced Persistent Threat (APT) Flax Typhoon*. Minētais *APT* izmantoja *Integrity Technology Group* produktus un tehnoloģijas, lai izvērstu savas datortīkla ekspluatācijas darbības. Pēc tam *Integrity Technology Group* produkti ir izmantoti, lai kompromitētu lietu interneta ierīces un piekļūtu tām dalībvalstīs, kā arī valstīs visā Eiropā un pasaulē. Laikposmā no 2022. līdz 2023. gadam *Flax Typhoon*, izmantojot *Integrity Technology Group* produktus, sešās dalībvalstīs piekļuva vismaz 65 600 lietu interneta ierīču. Tādējādi *Integrity Technology Group* komerciālie produkti un infrastruktūra tika regulāri izmantoti kiberuzbrukumos pret dalībvalstīm, kā arī pret trešām valstīm. Līdz ar to, ietekmējot informācijas sistēmas, kas saistītas ar digitālo infrastruktūru, *Integrity Technology Group* sniedz tehnisku un materiālu atbalstu kiberuzbrukumiem ar būtisku ietekmi, kas rada ārēju apdraudējumu dalībvalstīm un trešām valstīm.	16.3.2026.

	Nosaukums	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
6.	Emennet Pasargad	jeb: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten Reģistrācijas vieta: *Tehran*, Irāna Reģistrācijas Nr.: 554267 Galvenā uzņēmējdarbības vieta: *Tehran*, Irāna	*Emennet Pasargad* ir Irānas kiberaktors (uzņēmums), kas ir vērsies pret daudziem subjektiem, jo īpaši dalībvalstīs, kā arī Amerikas Savienotajās Valstīs (ASV). *Emennet Pasargad*, kas darbojas ar pieņemtu nosaukumu "*Anzu Team*", vērsās pret digitālo infrastruktūru Zviedrijā un apdraudēja Zviedrijas SMS pakalpojumu, ietekmējot lielu skaitu cilvēku. Turklāt, darbojoties ar pieņemtu nosaukumu "*Holy Souls*", šī vienība kompromitēja Francijas satīriskā žurnāla *Charlie Hebdo* abonentu datubāzi un reklamēja to pārdošanai tumšajā tīmeklī. *Emennet Pasargad* Parīzes Olimpisko spēļu laikā kompromitēja reklāmas stendus un izvietoja dezinformācijas kampaņas. *Emennet Pasargad*, apdraudot demokrātiju un tiesiskumu, arī mēģināja iejaukties ASV prezidenta vēlēšanās 2020. gadā, iegūstot konfidenciālu ASV vēlētāju informāciju un neatļautu piekļuvi ASV mediju uzņēmuma datortīklam. Tādējādi *Emennet Pasargad* ir atbildīgs par kiberuzbrukumiem ar būtisku ietekmi, kas rada ārēju apdraudējumu dalībvalstīm, un kiberuzbrukumiem ar būtisku ietekmi pret trešo valsti, un ir iesaistīts šādos uzbrukumos.	16.3.2026.

	Nosaukums	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
7.	Anxun Information Technology Co. Ltd.	安洵信息技术有限公司 (ķīniešu rakstībā) jeb: i-Soon Adrese: *Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai* Vienotais sociālā kredīta kods: 91510105332025597A (*Sichuan* birojs) Vienotais sociālā kredīta kods: 91310116561906136G (*Shanghai* birojs) Tīmekļa vietne: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win Tālruņa numuri: +862161119992, +8605645893417, +8613761671735, +864000665915 E-pasts: shutdown@163.com, isoon2015@126.com, tao_tingting@i-soon.net, li_ping@i-soon.net	*Anxun Information Technology Co. Ltd.* ir Ķīnas Tautas Republikā bāzēts uzņēmums, kas piedāvā "*hacking for-hire*" pakalpojumus. Tas ir vērsies pret dalībvalstu kritisko infrastruktūru un kritiskajām valsts funkcijām un piekļuvis klasificētai informācijai un to pārdevis. Turklāt *Anxun Information Technology Co. Ltd.* ir uzbrucis dažādu trešo valstu valdībām, tādējādi apdraudot Savienības kopējās ārpolitikas un drošības politikas (KĀDP) mērķus, kas izklāstīti Līguma par Eiropas Savienību 21. panta 2. punkta a) līdz c) apakšpunktā. *Anxun Information TechnologyCo. Ltd.* gūst būtisku ekonomisku labumu no sniegtajiem pakalpojumiem. Tādējādi *Anxun Information Technology Co. Ltd.* ir atbildīgs par kiberuzbrukumiem ar būtisku ietekmi, kas rada ārēju apdraudējumu dalībvalstīm, kā arī par kiberuzbrukumiem ar būtisku ietekmi pret trešām valstīm.	16.3.2026."