2026/589

16.3.2026

REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2026/589 AL CONSILIULUI

din 16 martie 2026

privind punerea în aplicare a Regulamentului (UE) 2019/796 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) 2019/796 al Consiliului din 17 mai 2019 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre [1], în special articolul 13 alineatul (1),

având în vedere propunerea Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate,

întrucât:

(1) La 17 mai 2019, Consiliul a adoptat Regulamentul (UE) 2019/796.

(2) Ca parte a acțiunii susținute, adaptate și coordonate a Uniunii împotriva entităților care reprezintă amenințări cibernetice persistente, două persoane fizice și trei entități ar trebui să fie incluse pe lista persoanelor fizice și juridice, a entităților și a organismelor cărora li se aplică măsurile restrictive prevăzută în anexa I la Regulamentul (UE) 2019/796. Respectivele persoane fizice și entități sunt răspunzătoare pentru atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre sau sunt implicate în astfel de atacuri.

(3) Prin urmare, anexa I la Regulamentul (UE) 2019/796 ar trebui să fie modificată în consecință,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Anexa I la Regulamentul (UE) 2019/796 se modifică în conformitate cu anexa la prezentul regulament.

Articolul 2

Prezentul regulament intră în vigoare la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 16 martie 2026.

Pentru Consiliu

Președintele

K. KALLAS

[1] JO L 129 I, 17.5.2019, p. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj.

ANEXĂ

Anexa I la Regulamentul (UE) 2019/796 se modifică după cum urmează:

1. în secțiunea „A. Persoane fizice” se adaugă următoarele rubrici:

	Nume	Informații de identificare	Motive	Data includerii pe listă
„18.	CHEN Cheng	陈诚 (ortografia chineză) Alias: Jesse Chen lengmo l3n6m0 Data nașterii: 20.10.1984 Locul nașterii: Yancheng, Jiangsu, China Cetățenia: chineză Sexul: masculin	Chen Cheng este un om de afaceri chinez, cofondator și unul dintre directorii generali (director general administrativ) ai Anxun Information Technology Co. Ltd. De asemenea, este reprezentant legal al sucursalei din Sichuan a respectivei societăți. Anxun Information Technology Co. Ltd., cunoscută și sub denumirea i-Soon, este o societate cu sediul în Republica Populară Chineză (RPC) care oferă servicii de tip «hacking-for-hire». Anxun Information Technology Co. Ltd. a vizat infrastructura critică și funcțiile critice ale statului din statele membre și a accesat și vândut informații clasificate. În plus, Anxun Information Technology Co. Ltd. a atacat guverne din diferite state terțe, ceea ce reprezintă o amenințare la adresa obiectivelor Uniunii în materie de politică externă și de securitate comună (PESC), astfel cum se prevede la articolul 21 alineatul (2) literele (a)-(c) din Tratatul privind Uniunea Europeană. Anxun Information Technology Co. Ltd. obține un beneficiu economic important din serviciile furnizate. Prin urmare, Anxun Information Technology Co. Ltd. este responsabilă de atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa statelor membre ale Uniunii, precum și de atacuri la adresa statelor terțe. În calitatea respectivă, Chen Cheng este responsabil de atacuri cibernetice cu efecte semnificative care reprezintă o amenințare externă la adresa statelor membre, precum și de atacuri cibernetice cu efecte semnificative împotriva unor state terțe și este implicat în astfel de atacuri.	16.3.2026

	Nume	Informații de identificare	Motive	Data includerii pe listă
19.	WU Haibo	吴海波 (ortografia chineză) Alias: shutdown shutd0wn Locul nașterii: China Cetățenia: chineză Sexul: masculin	Wu Haibo este un om de afaceri chinez, cofondator și unul dintre directorii generali (director general administrativ) ai Anxun Information Technology Co. Ltd. De asemenea, este reprezentant legal, președinte și director general al sucursalei din Shanghai («societatea mamă») a Anxun Information Technology Co. Ltd. De asemenea, acționează și în calitate de reprezentant legal al sucursalei din Sichuan al respectivei societăți. Anxun Information Technology Co. Ltd., cunoscută și sub denumirea i-Soon, este o societate cu sediul în Republica Populară Chineză (RPC) care oferă servicii de tip «hacking-for-hire». Anxun Information Technology Co. Ltd. a vizat infrastructura critică și funcțiile critice ale statului din statele membre și a accesat și vândut informații clasificate. În plus, Anxun Information Technology Co. Ltd. a atacat guverne din diferite state terțe, ceea ce reprezintă o amenințare la adresa obiectivelor Uniunii în materie de politică externă și de securitate comună (PESC), astfel cum se prevede la articolul 21 alineatul (2) literele (a)-(c) din Tratatul privind Uniunea Europeană. Anxun Information Technology Co. Ltd. obține un beneficiu economic important din serviciile furnizate. Prin urmare, Anxun Information Technology Co. Ltd. este responsabilă de atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa statelor membre, precum și de atacuri la adresa statelor terțe. Wu Haibo a fost implicat în conducerea și încurajarea tentativelor de atacuri cibernetice cu efecte semnificative asupra statelor membre. În calitatea respectivă, el este responsabil de atacuri cibernetice cu efecte semnificative care reprezintă o amenințare externă la adresa statelor membre, precum și de atacuri cibernetice cu efecte semnificative împotriva unor state terțe și este implicat în astfel de atacuri.	16.3.2026”;

2. în secțiunea „B. Persoane juridice, entități și organisme” se adaugă următoarele rubrici:

	Denumire	Informații de identificare	Motive	Data includerii pe listă
„5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (ortografia chineză) 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 Locul înregistrării: Beijing, China Data înregistrării: 2.9.2010 Codul unificat de credit social: 91110108562135265P	Integrity Technology Group este o întreprindere din domeniul securității cibernetice, cu sediul în Republica Populară Chineză (RPC), care a facilitat atacuri cibernetice legate de Advanced Persistent Threat – (APT) Flax Typhoon. Respectiva APT a utilizat produsele și tehnologia Integrity Technology Group pentru a-și desfășura activitățile de exploatare a rețelelor informatice. De atunci, produsele Integrity Technology Group au fost utilizate pentru a compromite și a accesa dispozitive din internetul obiectelor în statele membre, cât și în țări din întreaga Europă și la nivel global. Între 2022 și 2023, Flax Typhoon a accesat cel puțin 65 600 de dispozitive din internetul obiectelor în șase state membre prin utilizarea produselor Integrity Technology Group. Prin urmare, produsele comerciale și infrastructura Integrity Technology Group au fost utilizate în mod curent în atacurile cibernetice împotriva statelor membre, precum și a statelor terțe. În consecință, prin afectarea sistemelor informatice legate de infrastructura digitală, Integrity Technology Group oferă sprijin tehnic și material pentru atacurile cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa statelor membre și a statelor terțe.	16.3.2026

	Denumire	Informații de identificare	Motive	Data includerii pe listă
6.	Emennet Pasargad	Alias: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten Locul înregistrării: Teheran, Iran Număr de înregistrare: 554267 Locul principal de desfășurare a activității: Teheran, Iran	Emennet Pasargad este un actor cibernetic iranian (societate) care a vizat numeroase entități, în special în statele membre, precum și în Statele Unite (SUA). Emennet Pasargad, care acționează sub denumirea «Anzu Team», a vizat infrastructura digitală din Suedia și a compromis un serviciu SMS suedez, afectând un număr mare de persoane. În plus, acționând sub denumirea «Holy Souls», entitatea a compromis baza de date a abonaților revistei satirice franceze Charlie Hebdo și a oferit-o spre vânzare pe dark web. Emennet Pasargard a compromis panourile publicitare în timpul Jocurilor Olimpice de la Paris și a afișat campanii de dezinformare. Emennet Pasargad a încercat, de asemenea, să intervină în alegerile prezidențiale din SUA în 2020, amenințând democrația și statul de drept, obținând informații confidențiale despre alegătorii americani și obținând acces neautorizat la rețeaua informatică a unei societăți mass-media din SUA. Prin urmare, Emennet Pasargad este responsabil de atacuri cibernetice cu efecte semnificative care reprezintă o amenințare externă la adresa statelor membre, precum și de atacuri cibernetice cu efecte semnificative împotriva unui stat terț.	16.3.2026

	Denumire	Informații de identificare	Motive	Data includerii pe listă
7.	Anxun Information Technology Co. Ltd.	安洵信息技术有限公司 (ortografia chineză) Alias: i-Soon Adresa: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai Codul unificat de credit social: 91510105332025597A (sucursala din Sichuan) Codul unificat de credit social: 91310116561906136G (sucursala din Shanghai) Site web: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win Numere de telefon: +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. este o societate cu sediul în Republica Populară Chineză care oferă servicii de tip «hacking-for-hire». Aceasta a vizat infrastructura critică și funcțiile critice ale statului din statele membre și a accesat și vândut informații clasificate. În plus, Anxun Information Technology Co. Ltd. a atacat guverne din diferite state terțe, ceea ce reprezintă o amenințare la adresa obiectivelor Uniunii în materie de politică externă și de securitate comună (PESC), astfel cum se prevede la articolul 21 alineatul (2) literele (a)-(c) din Tratatul privind Uniunea Europeană. Anxun Information Technology Co. Ltd. obține un beneficiu economic important din serviciile furnizate. Prin urmare, Anxun Information Technology Co. Ltd. este responsabilă de atacuri cibernetice cu efecte semnificative care reprezintă o amenințare externă la adresa statelor membre, precum și de atacuri cibernetice cu efecte semnificative împotriva unor state terțe.	16.3.2026”.

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