2026/589

16.3.2026 г.

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2026/589 НА СЪВЕТА

от 16 март 2026 година

за прилагане на Регламент (ЕС) 2019/796 относно ограничителни мерки срещу кибератаки, застрашаващи Съюза или неговите държави членки

СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) 2019/796 на Съвета от 17 май 2019 г. относно ограничителни мерки срещу кибератаки, застрашаващи Съюза или неговите държави членки ([1]), и по-специално член 13, параграф 1 от него,

като взе предвид предложението на върховния представител на Съюза по въпросите на външните работи и политиката на сигурност,

като има предвид, че:

(1) На 17 май 2019 г. Съветът прие Регламент (ЕС) 2019/796.

(2) Като част от непрекъснатите, целенасочени и координирани действия на Съюза срещу упорстващите извършители на киберзаплахи, в списъка на подложените на ограничителни мерки физически и юридически лица, образувания и органи, съдържащ се в приложение I към Регламент (ЕС) 2019/796, следва да бъдат включени две физически лица и три образувания. Тези физически лица и образувания са отговорни или участват в кибератаки със значително въздействие, които представляват външна заплаха за Съюза или за неговите държави членки.

(3) Поради това приложение I към Регламент (ЕС) 2019/796 следва да бъде съответно изменено,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Приложение I към Регламент (ЕС) 2019/796 се изменя в съответствие с приложението към настоящия регламент.

Член 2

Настоящият регламент влиза в сила в деня на публикуването му в *Официален вестник на Европейския съюз*.

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на 16 март 2026 година.

За Съвета

Председател

K. KALLAS

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

ПРИЛОЖЕНИЕ

Приложение I към Регламент (ЕС) 2019/796 се изменя, както следва:

1) В раздел „A. Физически лица“ се добавят следните вписвания:

	Име	Идентификационни данни	Основания	Дата на вписване
„18.	CHEN Cheng	陈诚 (изписване на китайски език) Изв. още като: Jesse Chen lengmo l3n6m0 Дата на раждане: 20.10.1984 г. Място на раждане: Yancheng, Jiangsu, Китай Гражданство: китайско Пол: мъжки	Chen Cheng е китайски бизнесмен, съосновател и един от генералните директори на Anxun Information Technology Co. Ltd. Той е и законен представител на клона на въпросното дружество в Съчуан. Anxun Information Technology Co. Ltd., известно още като i-Soon, е дружество със седалище в Китайската народна република (КНР), което предлага услугите „хакерски атаки по поръчка“. Anxun Information Technology Co. Ltd. е имало за мишена критичната инфраструктура и критичните държавни функции на държавите членки, и е осъществявало достъп до класифицирана информация, която е продавало. Освен това Anxun Information Technology Co. Ltd е атакувало правителства на различни трети държави, създавайки по този начин опасност за целите на Съюза, свързани с общата външна политика и политика на сигурност (ОВППС), съгласно член 21, параграф 2, букви а—в от Договора за Европейския съюз. Anxun Information Technology Co. Ltd. извлича значителна икономическа полза от предоставяните услуги. Следователно Anxun Information Technology Co. Ltd. е отговорно за кибератаки със значително въздействие, представляващи външна заплаха за Съюза и неговите държави членки, както и за атаки срещу трети държави. В това си качество Chen Cheng е отговорен и участва в кибератаки със значително въздействие, които представляват външна заплаха за държавите членки, както и в кибератаки със значително въздействие срещу трети държави.	16.3.2026 г.

	Име	Идентификационни данни	Основания	Дата на вписване
19.	WU Haibo	吴海波 (изписване на китайски език) Изв. още като: shutdown shutd0wn Място на раждане: Китай Гражданство: китайско Пол: мъжки	Wu Haibo е китайски бизнесмен, съосновател и един от генералните директори на Anxun Information Technology Co. Ltd. Той също така е законен представител, председател и генерален директор на клона в Шанхай („клона майка“) на Anxun Information Technology Co. Ltd. Освен това, той действа и като законен представител на клона на това дружество в Съчуан. Anxun Information Technology Co. Ltd., известно още като i-Soon, е дружество със седалище в Китайската народна република (КНР), което предлага услугите „хакерски атаки по поръчка“. Anxun Information Technology Co. Ltd. е имало за мишена критичната инфраструктура и критичните държавни функции на държавите членки. и е осъществявало достъп до класифицирана информация, която е продавало. Освен това Anxun Information Technology Co. Ltd. е атакувало правителства на различни трети държави, създавайки по този начин опасност за целите на Съюза, свързани с общата външна политика и политика на сигурност (ОВППС), съгласно член 21, параграф 2, букви а—в от Договора за Европейския съюз. Anxun Information Technology Co. Ltd. извлича значителна икономическа полза от предоставяните услуги. Следователно Anxun Information Technology Co. Ltd. е отговорно за кибератаки със значително въздействие, които представляват външна заплаха за държавите членки, както и за атаки срещу трети държави. Wu Haibo е участвал в ръководенето и насърчаването на опити за кибератаки със значително въздействие срещу държавите членки. В това си качество той е отговорен и участва в кибератаки със значително въздействие, които представляват външна заплаха за държавите членки, както и в кибератаки със значително въздействие срещу трети държави.	16.3.2026 г.“

2) В раздел „Б. Юридически лица, образувания и органи“ се добавят следните вписвания:

	Наименование	Идентификационни данни	Основания	Дата на вписване
„5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (изписване на китайски език) Изв. още като: Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited Адрес: Fenghao East Road, Room 103, Building 6, No. 9, Beijing Haidian District, China Място на регистрация: Пекин, Китай Дата на регистрация: 2.9.2010 г. Единен търговско-данъчен регистрационен номер: 91110108562135265P	Integrity Technology Group е предприятие в областта на киберсигурността със седалище в Китайската народна република (КНР), което улеснява кибератаки, свързани с Advanced Persistent Threat (APT) Flax Typhoon. Въпросната APT е използвала продуктите и технологиите на Integrity Technology Group за разгръщане на дейностите си, свързани с експлоатацията на компютърните мрежи. Оттогава насам продуктите на Integrity Technology Group се използват за компрометиране и достъп до устройства за интернет на предметите в държавите членки, както и в държавите в Европа и и в световен мащаб. Между 2022 г. и 2023 г. Flax Typhoon е получил достъп до най-малко 65 600 устройства за интернет на предметите в шест държави членки, като са използвали продуктите на Integrity Technology Group. Поради това търговските продукти и инфраструктура на Integrity Technology Group са били използвани рутинно при кибератаки срещу държави членки и срещу трети държави. Следователно, като засяга информационните системи, свързани с цифровата инфраструктура, Integrity Technology Group предоставя техническа и материална подкрепа за кибератаки със значително въздействие, които представляват външна заплаха за държавите членки и трети държави.	16.3.2026 г.

	Наименование	Идентификационни данни	Основания	Дата на вписване
6.	Emennet Pasargad	Изв. още като: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten Място на регистрация: Техеран, Иран Регистрационен номер: 554267 Основно място на стопанска дейност: Техеран, Иран	Emennet Pasargad е ирански извършител на кибератаки (дружество), чиято мишена са множество образувания, по-специално в държавите членки, както и в Съединените щати (САЩ). Emennet Pasargad, работещо под псевдонима Anzu Team, е взело на прицел цифрова инфраструктура в Швеция и е компрометирало шведска услуга за SMS, засягаща голям брой хора. Освен това, действайки под псевдонима Holy Souls, образуването е компрометирало базата данни на абонатите на френското сатирично списание „Шарли Ебдо“ и ги е рекламирало с цел продажба в тъмната мрежа. Emennet Pasargad е компрометирало рекламни билбордове по време на Олимпийските игри в Париж и е водело кампании за дезинформация. Emennet Pasargad също така се е опитвало да се намеси в президентските избори в САЩ през 2020 г., застрашавайки демокрацията и принципите на правовата държава, като получава поверителна информация за американските гласоподаватели и неразрешен достъп до компютърната мрежа на американско медийно дружество. Следователно Emennet Pasargad е отговорно за кибератаки със значително въздействие, които представляват външна заплаха за държавите членки, както и за кибератаки със значително въздействие срещу трета държава.	16.3.2026 г.

	Наименование	Идентификационни данни	Основания	Дата на вписване
7.	Anxun Information Technology Co. Ltd.	安洵信息技术有限公司 (изписване на китайски език) Изв. още като: I-Soon Адрес: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai Единен търговско-данъчен регистрационен номер: 91510105332025597A (клон в Съчуан) Единен търговско-данъчен регистрационен номер: 91310116561906136G (клон в Шанхай) Уебсайт: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win Телефонни номера: +862161119992, +8605645893417, +8613761671735, +864000665915 Email: shutdown@163.com, isoon2015@126.com, tao_tingting@i-soon.net, li_ping@i-soon.net	Anxun Information Technology Co. Ltd. е дружество със седалище в Китайската народна република, което предлага услугите „хакерски атаки по поръчка“. Негова мишена са критичната инфраструктура и критичните държавни функции на държавите членки. То е осъществявало достъп до класифицирана информация, която е продавало. Освен това Anxun Information Technology Co. Ltd. е атакувало правителства на различни трети държави, създавайки по този начин опасност за целите на Съюза, свързани с общата външна политика и политика на сигурност (ОВППС), съгласно член 21, параграф 2, букви а—в от Договора за Европейския съюз. Anxun Information Technology Co. Ltd. извлича значителна икономическа полза от предоставяните услуги. Следователно Anxun Information Technology Co. Ltd. е отговорно за кибератаки със значително въздействие, които представляват външна заплаха за държавите членки, както и за кибератаки със значително въздействие срещу трети държави.	16.3.2026 г.“.