2026/589

16.3.2026

REGULAMENTO DE EXECUÇÃO (UE) 2026/589 DO CONSELHO

de 16 de março de 2026

que dá execução ao Regulamento (UE) 2019/796 relativo a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros

O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o Regulamento (UE) 2019/796 do Conselho, de 17 de maio de 2019, relativo a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros ([1]), nomeadamente o artigo 13.º, n. 1,

Tendo em conta a proposta da alta representante da União para os Negócios Estrangeiros e a Política de Segurança,

Considerando o seguinte:

(1) Em 17 de maio de 2019, o Conselho adotou o Regulamento (UE) 2019/796.

(2) No âmbito da ação sustentada, adaptada e coordenada da União contra os responsáveis por ciberameaças persistentes, duas pessoas singulares e três entidades deverão ser incluídas na lista de pessoas singulares e coletivas, entidades e organismos sujeitos a medidas restritivas constante do anexo I do Regulamento (UE) 2019/796. Essas pessoas singulares e entidades são responsáveis ou estão envolvidas em ciberataques com um efeito significativo, que constituem uma ameaça externa para a União ou os seus Estados-Membros.

(3) Por conseguinte, o anexo I do Regulamento (UE) 2019/796 deverá ser alterado em conformidade,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

O anexo I do Regulamento (UE) 2019/796 é alterado nos termos do anexo do presente regulamento.

Artigo 2.º

O presente regulamento entra em vigor no dia da sua publicação no *Jornal Oficial da União Europeia*.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Feito em Bruxelas, em 16 de março de 2026.

Pelo Conselho

A Presidente

K. KALLAS

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

ANEXO

O anexo I do Regulamento (UE) 2019/796 é alterado do seguinte modo:

1) São aditadas as seguintes entradas à rubrica «A. Pessoas singulares»:

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
«18.	CHEN Cheng	陈诚 (grafia chinesa) Pseudónimos: Jesse Chen lengmo l3n6m0 Data de nascimento: 20.10.1984 Local de nascimento: Yancheng, Jiangsu, China Nacionalidade: chinesa Sexo: masculino	Chen Cheng é um empresário chinês, cofundador e um dos diretores gerais (diretor de operações) da Anxun Information Technology Co. Ltd. É também um representante legal da sucursal de Sichuan da empresa. A Anxun Information Technology Co. Ltd., também conhecida por i-Soon, é uma empresa sediada na República Popular da China que oferece serviços de "pirataria informática". A Anxun Information Technology Co. Ltd. atacou infraestruturas críticas e funções cruciais de um Estado de Estados-Membros e acedeu a informações classificadas, tendo-as vendido. Além disso, a Anxun Information Technology Co. Ltd. atacou governos de vários Estados terceiros, constituindo assim uma ameaça para os objetivos da política externa e de segurança comum (PESC) da União, tal como enunciados no artigo 21. º, n. º 2, alíneas a) a c), do Tratado da União Europeia. A Anxun Information Technology Co. Ltd. obtém um importante benefício económico dos serviços prestados Por conseguinte, a Anxun Information Technology Co. Ltd. é responsável por ciberataques com efeitos significativos, que constituem uma ameaça externa para a União e os seus Estados-Membros, bem como ataques contra Estados terceiros. Nessa qualidade, Chen Cheng é responsável e está implicado em ciberataques com efeitos significativos, que constituem uma ameaça externa para os Estados-Membros, bem como em ciberataques com um efeito significativo contra Estados terceiros.	16.3.2026

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
19.	WU Haibo	吴海波 (grafia chinesa) Pseudónimos: shutdown shutd0wn Local de nascimento: China Nacionalidade: chinesa Sexo: masculino	Wu Haibo é um empresário chinês, cofundador e um dos diretores gerais (diretor executivo) da Anxun Information Technology Co. Ltd. É também representante legal, presidente e diretor-geral da sucursal de Xangai ("empresa-mãe") da Anxun Information Technology Co. Ltd. Para além disso, atua também como representante legal da sucursal de Sichuan dessa empresa. A Anxun Information Technology Co. Ltd., também conhecida por i-Soon, é uma empresa sediada na República Popular da China que oferece serviços de "pirataria informática". A Anxun Information Technology Co. Ltd.atacou infraestruturas críticas e funções cruciais de um Estado de Estados-Membros e acedeu a informações classificadas, tendo-as vendido. Além disso, a Anxun Information Technology atacou governos de vários Estados terceiros, constituindo assim uma ameaça para os objetivos da política externa e de segurança comum (PESC) da União, tal como enunciados no artigo 21. º, n. º 2, alíneas a) a c), do Tratado da União Europeia. A Anxun Information Technology Co. Ltd. obtém um importante benefício económico dos serviços prestados. Por conseguinte, a Anxun Information Technology é responsável por ciberataques com efeitos significativos, que constituem uma ameaça externa para os Estados-Membros, bem como contra Estados terceiros. Wu Haibo esteve implicado na direção e no incentivo a tentativas de ciberataques com um efeito significativo contra Estados-Membros. Nessa qualidade, é responsável e está implicado em ciberataques com efeitos significativos, que constituem uma ameaça externa para os Estados-Membros, bem como em ciberataques com efeitos significativos contra Estados terceiros.	16.3.2026»;

2) São aditadas as seguintes entradas à rubrica «B. Pessoas coletivas, entidades e organismos»:

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
«5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (grafia chinesa) Pseudónimos: Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited Endereço: Fenghao East Road, Room 103, Building 6, N.º 9, Beijing Haidian District, China Local de registo: Pequim, China Data de registo: 2.9.2010 Código Unificado de Crédito Social: 91110108562135265P	A Integrity Technology Group é uma empresa de cibersegurança, sediada na República Popular da China (RPC), que facilitou ciberataques relacionados com o Advanced Persistent Threat (APT) Flax Typhoon. Esse APT usou os produtos e a tecnologia da Integrity Technology Group para levar a cabo as suas atividades de exploração de redes informáticas. Desde então, os produtos da Integrity Technology Group têm sido utilizados para comprometer e aceder a dispositivos da Internet das coisas nos Estados-Membros, em países por toda a Europa e em todo o mundo. Entre 2022 e 2023, a a Flax Typhoon acedeu a, pelo menos, 65 600 dispositivos da Internet das coisas em seis Estados-Membros usando produtos da Integrity Technology Group. Por conseguinte, os produtos e infraestruturas comerciais da Integrity Technology Group foram usados regularmente em ciberataques contra Estados-Membros e países terceiros. Consequentemente, ao afetar sistemas de informação relacionados com infraestruturas digitais, a Integrity Technology Group presta apoio técnico e material a ciberataques com efeitos significativos, que constituem uma ameaça externa para os Estados-Membros e Estados terceiros.	16.3.2026

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
6.	Emennet Pasargad	Pseudónimos: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten Local de registo: Teerão, Irão Número de registo: 554267 Estabelecimento principal: Teerão, Irão	Emennet Pasargad é um interveniente (empresa) iraniano no domínio cibernético que atacou numerosas entidades, nomeadamente em Estados-Membros e nos Estados Unidos. Emennet Pasargard, que opera sob o pseudónimo "Anzu Team", atacou infraestruturas digitais na Suécia e comprometeu um serviço sueco de SMS, afetando um grande número de pessoas. Além disso, atuando sob o pseudónimo "Holy Souls", a entidade comprometeu a base de dados de assinantes da revista satírica francesa Charlie Hebdo, tendo-a publicitado para venda na Web obscura. Emennet Pasargard comprometeu painéis publicitários durante os Jogos Olímpicos de Paris e levou a cabo campanhas de desinformação. Emennet Pasargard tentou também interferir nas eleições presidenciais de 2020 nos Estados Unidos, ameaçando a democracia e o Estado de direito, obtendo informações confidenciais sobre os eleitores americanos e obtendo acesso não autorizado à rede informática de uma empresa de comunicação social dos Estados Unidos. Por conseguinte, Emennet Pasargard é responsável por ciberataques com efeitos significativos, que constituem uma ameaça externa para os Estados-Membros, e por ciberataques com efeitos significativos contra um Estado terceiro.	16.3.2026

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
7.	Anxun Information Technology Co. Ltd	安洵信息技术有限公司 (grafia chinesa) Pseudónimos: I-Soon Endereço: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai Código Unificado de Crédito Social: 91510105332025597A (sucursal de Sichuan) Código Unificado de Crédito Social: 91310116561906136G (sucursal de Xangai) Sítio Web: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win Números de telefone: +862161119992, +8605645893417, +8613761671735, +864000665915 Endereço eletrónico: shutdown@163.com, isoon2015@126.com, tao_tingting@i-soon.net, li_ping@i-soon.net	A Anxun Information Technology Co. Ltd. é uma empresa sediada na República Popular da China que oferece serviços de "pirataria informática". Atacou infraestruturas críticas e funções cruciais de um Estado de Estados-Membros e acedeu a informações classificadas, tendo-as vendido. Além disso, a Anxun Information Technology Co. Ltd. atacou governos de vários Estados terceiros, constituindo assim uma ameaça para os objetivos da política externa e de segurança comum (PESC) da União, tal como enunciados no artigo 21. º, n. º 2, alíneas a) a c), do Tratado da União Europeia. A Anxun Information Technology Co. Ltd. obtém um importante benefício económico dos serviços prestados. Por conseguinte, a Anxun Information Technology Co. Ltd. é responsável por ciberataques com efeitos significativos, que constituem uma ameaça externa para os Estados-Membros, bem como por ciberataques com efeitos significativos contra Estados terceiros.	16.3.2026».