Publicatieblad
van de Europese Unie

NL
L-serie

2026/589

16.3.2026

UITVOERINGSVERORDENING (EU) 2026/589 VAN DE RAAD

van 16 maart 2026

tot uitvoering van Verordening (EU) 2019/796 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen

DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) 2019/796 van de Raad van 17 mei 2019 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen ([1]), en met name artikel 13, lid 1,

Gezien het voorstel van de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid,

Overwegende hetgeen volgt:

(1) Op 17 mei 2019 heeft de Raad Verordening (EU) 2019/796 vastgesteld.

(2) In het kader van het volgehouden, op maat gesneden en gecoördineerde optreden van de Unie tegen actoren die aanhoudend voor cyberdreigingen zorgen, moeten twee natuurlijke personen en drie entiteiten worden toegevoegd aan de in bijlage I bij Verordening (EU) 2019/796 opgenomen lijst van natuurlijke personen en rechtspersonen, entiteiten en lichamen die aan beperkende maatregelen onderworpen zijn. Die natuurlijke personen en entiteiten zijn verantwoordelijk voor of betrokken bij cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de Unie of haar lidstaten.

(3) Bijlage I bij Verordening (EU) 2019/796 moet derhalve dienovereenkomstig worden gewijzigd,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Bijlage I bij Verordening (EU) 2019/796 wordt gewijzigd overeenkomstig de bijlage bij deze verordening.

Artikel 2

Deze verordening treedt in werking op de datum van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 16 maart 2026.

Voor de Raad

De voorzitter

K. KALLAS

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

BIJLAGE

Bijlage I bij Verordening (EU) 2019/796 wordt als volgt gewijzigd:

1) de volgende vermeldingen worden toegevoegd aan rubriek “A. Natuurlijke personen”:

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
“18.	CHEN Cheng	陈诚 (Chinese spelling) Alias: Jesse Chen lengmo l3n6m0 Geboortedatum: 20.10.1984 Geboorteplaats: Yancheng, Jiangsu, China Nationaliteit: Chinese Geslacht: mannelijk	Chen Cheng is een Chinese zakenman, medeoprichter en een van de algemeen directeuren (*Chief Operating Officer*) van Anxun Information Technology Co. Ltd. Hij is ook een wettelijke vertegenwoordiger van het filiaal van die onderneming in Sichuan. Anxun Information Technology Co. Ltd., ook bekend als i-Soon, is een in de Volksrepubliek China (VRC) gevestigd bedrijf dat “hacking-for-hire”-diensten aanbiedt. Anxun Information Technology Co. Ltd.heeft gericht kritieke infrastructuur en kritieke staatsfuncties van lidstaten aangevallen en toegang verkregen tot gerubriceerde informatie en deze verkocht. Bovendien heeft Anxun Information Technology Co. Ltd. de regeringen van verschillende derde landen aangevallen, hetgeen een bedreiging vormt voor de doelstellingen van het gemeenschappelijk buitenlands en veiligheidsbeleid (GBVB) van de Unie, zoals uiteengezet in artikel 21, lid 2, punten a) tot en met c), van het Verdrag betreffende de Europese Unie. Anxun Information Technology Co. Ltd. haalt een belangrijk economisch voordeel uit de verleende diensten. Anxun Information Technology Co. Ltd. is derhalve verantwoordelijk voor cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de Unie en haar lidstaten, alsook aanvallen tegen derde landen. In deze hoedanigheid is Chen Cheng verantwoordelijk voor en betrokken bij cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de lidstaten, alsook cyberaanvallen tegen derde landen met aanzienlijke gevolgen.	16.3.2026

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
19.	WU Haibo	吴海波 (Chinese spelling) Alias: shutdown shutd0wn Geboorteplaats: China Nationaliteit: Chinese Geslacht: mannelijk	Wu Haibo is een Chinese zakenman, medeoprichter en een van de algemeen directeuren (*Chief Executive Officer*) van Anxun Information Technology Co. Ltd. Hij is ook de wettelijke vertegenwoordiger, voorzitter en algemeen directeur van het filiaal in Shanghai ("moederbedrijf") van Anxun Information Technology Co. Ltd. Bovendien treedt hij op als de wettelijke vertegenwoordiger van het filiaal van die onderneming in Sichuan. Anxun Information Technology Co. Ltd., ook bekend als i-Soon, is een in de Volksrepubliek China (VRC) gevestigd bedrijf dat "hacking-for-hire"-diensten aanbiedt. Het heeft gericht kritieke infrastructuur en kritieke staatsfuncties van lidstaten aangevallen en toegang verkregen tot gerubriceerde informatie en deze verkocht. Bovendien heeft Anxun Information Technology Co. Ltd. de regeringen van verschillende derde landen aangevallen, hetgeen een bedreiging vormt voor de doelstellingen van het gemeenschappelijk buitenlands en veiligheidsbeleid (GBVB) van de Unie, zoals uiteengezet in artikel 21, lid 2, punten a) tot en met c), van het Verdrag betreffende de Europese Unie. Anxun Information Technology Co. Ltd. haalt een belangrijk economisch voordeel uit de verleende diensten. Anxun Information Technology Co. Ltd. is derhalve verantwoordelijk voor cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de lidstaten, alsook aanvallen tegen derde landen. Wu Haibo was betrokken bij het aansturen en aanmoedigen van pogingen tot cyberaanvallen tegen lidstaten met een aanzienlijk gevolg. In deze hoedanigheid is hij verantwoordelijk voor en betrokken bij cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de lidstaten, alsook cyberaanvallen tegen derde landen met aanzienlijke gevolgen.	16.3.2026"

2) de volgende vermeldingen worden toegevoegd aan rubriek “B. Rechtspersonen, entiteiten en lichamen”:

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
“5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (Chinese spelling) Ook bekend als: Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited Adres: Fenghao East Road, Room 103, Building 6, No. 9, Beijing Haidian District, China (Peking, China) Plaats van registratie: Peking, China Registratiedatum: 2.9.2010 Unified Social Credit Code: 91110108562135265P	Integrity Technology Group is een in de Volksrepubliek China (VRC) gevestigd cyberbeveiligingsbedrijf dat cyberaanvallen heeft gefaciliteerd in verband met de geavanceerde aanhoudende dreiging (*Advanced Persistent Threat* – APT) Flax Typhoon. Die APT gebruikte de producten en de technologie van Integrity Technology Group om zijn activiteiten op het gebied van de exploitatie van computernetwerken uit te rollen. De producten van Integrity Technology Group worden sindsdien gebruikt om met het internet der dingen verbonden apparaten in de lidstaten, alsook in landen in heel Europa en mondiaal te compromitteren en er toegang toe te krijgen. Flax Typhoon heeft zich tussen 2022 en 2023 in zes lidstaten toegang verschaft tot ten minste 65 600 met het internet der dingen verbonden apparaten door gebruik te maken van producten van Integrity Technology Group. De commerciële producten en de infrastructuur van Integrity Technology Group werden daarom regelmatig gebruikt bij cyberaanvallen tegen lidstaten en derde landen. Door informatiesystemen met betrekking tot digitale infrastructuur aan te vallen, verleent Integrity Technoglogy Group bijgevolg technische en materiële steun voor cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de lidstaten en derde landen.	16.3.2026

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
6.	Emennet Pasargad	Ook bekend als: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten Plaats van registratie: Teheran, Iran Registratienummer: 554267 Voornaamste plaats van bedrijvigheid: Teheran, Iran	Emennet Pasargad is een Iraanse cyberactor (bedrijf) die tal van entiteiten gericht heeft aangevallen, met name in de lidstaten en in de Verenigde Staten (VS). Emennet Pasargad heeft onder de alias “Anzu Team” gericht digitale infrastructuur in Zweden aangevallen en heeft een Zweedse sms-dienst gecompromitteerd, waardoor een groot aantal personen werd getroffen. Bovendien heeft de entiteit, onder de alias “Holy Souls”, het abonneebestand van het Franse satirische tijdschrift Charlie Hebdo gecompromitteerd en op het darkweb te koop aangeboden. Emennet Pasargad heeft tijdens de Olympische Spelen van Parijs reclameborden gehackt en desinformatiecampagnes op touw gezet. Emennet Pasargad probeerde ook de Amerikaanse presidentsverkiezingen van 2020 te beïnvloeden – wat een bedreiging is van de democratie en de rechtsstaat – door vertrouwelijke informatie over Amerikaanse kiezers te vergaren en zich ongeoorloofde toegang te verschaffen tot het computernetwerk van een Amerikaans mediabedrijf. Emennet Pasargad is derhalve verantwoordelijk voor cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de lidstaten, en voor cyberaanvallen tegen een derde land met aanzienlijke gevolgen.	16.3.2026

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
7.	Anxun Information Technology Co. Ltd.	安洵信息技术有限公司 (Chinese spelling) Ook bekend als: i-Soon Adres: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai (China) Unified Social Credit Code: 91510105332025597A (filiaal Sichuan) Unified Social Credit Code: 91310116561906136G (filiaal Shanghai) Website: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win Telefoonnummers: +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. is een in de Volksrepubliek China gevestigd bedrijf dat "hacking-for-hire"-diensten aanbiedt. Het heeft gericht kritieke infrastructuur en kritieke staatsfuncties van lidstaten aangevallen en toegang verkregen tot gerubriceerde informatie en deze verkocht. Bovendien heeft Anxun Information Technology Co. Ltd. de regeringen van verschillende derde landen aangevallen, hetgeen een bedreiging vormt voor de doelstellingen van het gemeenschappelijk buitenlands en veiligheidsbeleid (GBVB) van de Unie, zoals uiteengezet in artikel 21, lid 2, punten a) tot en met c), van het Verdrag betreffende de Europese Unie. Anxun Information Technology Co. Ltd. haalt een belangrijk economisch voordeel uit de verleende diensten. Anxun Information Technology Co. Ltd. is derhalve verantwoordelijk voor cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de lidstaten, alsook voor cyberaanvallen tegen derde landen met aanzienlijke gevolgen.	16.3.2026"