Amtsblatt
der Europäischen Union

DE
Reihe L

2026/589

16.3.2026

DURCHFÜHRUNGSVERORDNUNG (EU) 2026/589 DES RATES

vom 16. März 2026

zur Durchführung der Verordnung (EU) 2019/796 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen

DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2019/796 des Rates vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen [1], insbesondere auf Artikel 13 Absatz 1,

auf Vorschlag der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik,

in Erwägung nachstehender Gründe:

(1) Der Rat hat am 17. Mai 2019 die Verordnung (EU) 2019/796 angenommen.

(2) Als Teil dauerhafter, maßgeschneiderter und koordinierter Maßnahmen der Union gegen Akteure, von denen eine anhaltende Cyberbedrohung ausgeht, sollten zwei natürliche Personen und drei Organisationen in die in Anhang I der Verordnung (EU) 2019/796 enthaltenen Liste der natürlichen und juristischen Personen, Organisationen und Einrichtungen, gegen die restriktive Maßnahmen verhängt wurden, aufgenommen werden. Diese natürlichen Personen und Organisationen sind für Cyberangriffe mit erheblichen Auswirkungen, die eine äußere Bedrohung für die Union oder ihre Mitgliedstaaten darstellen, verantwortlich oder daran beteiligt.

(3) Anhang I der Verordnung (EU) 2019/796 sollte daher entsprechend geändert werden —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Anhang I der Verordnung (EU) 2019/796 wird gemäß dem Anhang der vorliegenden Verordnung geändert.

Artikel 2

Diese Verordnung tritt am Tag ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu Brüssel am 16. März 2026.

Im Namen des Rates

Die Präsidentin

K. KALLAS

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

ANHANG

Anhang I der Verordnung (EU) 2019/796 wird wie folgt geändert:

1. Folgende Einträge werden unter der Überschrift „A. Natürliche Personen“ angefügt:

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
„18.	Chen Cheng	陈诚 (chinesische Schreibweise) Aliasnamen: Jesse Chen lengmo l3n6m0 Geburtsdatum: 20.10.1984 Geburtsort: Yancheng, Jiangsu, China Staatsangehörigkeit: chinesisch Geschlecht: männlich	Chen Cheng ist ein chinesischer Geschäftsmann, Mitbegründer und einer der Geschäftsführer (Chief Operating Officer) von Anxun Information Technology Co. Ltd. Er ist auch ein gesetzlicher Vertreter der Zweigniederlassung des Unternehmens in Sichuan. Anxun Information Technology Co. Ltd., auch bekannt als i-Soon, ist ein in der Volksrepublik China (VR China) ansässiges Unternehmen, das ‚Hack-for-hire‘-Dienstleistungen anbietet. Anxun Information Technology Co. Ltd hat gezielt kritische Infrastrukturen und kritische staatliche Funktionen der Mitgliedstaaten angegriffen sowie auf Verschlusssachen zugegriffen und diese verkauft. Darüber hinaus hat Anxun Information Technology Co. Ltd. die Regierungen verschiedener Drittstaaten angegriffen und stellt damit eine Bedrohung für die Ziele der Gemeinsamen Außen- und Sicherheitspolitik (GASP) der Union gemäß Artikel 21 Absatz 2 Buchstaben a bis c des Vertrags über die Europäische Union dar. Anxun Information Technology Co. Ltd. profitiert wirtschaftlich erheblich von den erbrachten Dienstleistungen. Anxun Information Technology Co. Ltd. ist daher für Cyberangriffe mit erheblichen Auswirkungen verantwortlich, die eine äußere Bedrohung für die Union und ihre Mitgliedstaaten darstellen, sowie für Angriffe auf Drittstaaten. In dieser Funktion ist Chen Cheng für Cyberangriffe mit erheblichen Auswirkungen, die eine äußere Bedrohung für die Mitgliedstaaten darstellen, sowie für Cyberangriffe mit erheblichen Auswirkungen auf Drittstaaten verantwortlich und an diesen beteiligt.	16.3.2026

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
19.	Wu Haibo	吴海波 (chinesische Schreibweise) Aliasnamen: shutdown shutd0wn Geburtsort: China Staatsangehörigkeit: chinesisch Geschlecht: männlich	Wu Haibo ist ein chinesischer Geschäftsmann, Mitbegründer und einer der Geschäftsführer (Chief Executive Officer) von Anxun Information Technology Co. Ltd. Er ist auch gesetzlicher Vertreter, Vorsitzender und Geschäftsführer der Niederlassung von Anxun Information Technology Co. Ltd in Shanghai („Mutterschiff"). Er handelt auch als gesetzlicher Vertreter der Zweigniederlassung in Sichuan dieses Unternehmens. Anxun Information Technology Co. Ltd., auch bekannt als i-Soon, ist ein in der Volksrepublik China (VR China) ansässiges Unternehmen, das „Hack-for-hire"-Dienstleistungen anbietet. Anxun Information Technology Co. Ltd hat gezielt kritische Infrastrukturen und kritische staatliche Funktionen der Mitgliedstaaten angegriffen sowie auf Verschlusssachen zugegriffen und diese verkauft. Darüber hinaus hat Anxun Information Technology Co. Ltd.die Regierungen verschiedener Drittstaaten angegriffen und damit eine Bedrohung für die Ziele der Gemeinsamen Außen- und Sicherheitspolitik (GASP) der Union gemäß Artikel 21 Absatz 2 Buchstaben a bis c des Vertrags über die Europäische Union dargestellt. Anxun Information Technology Co. Ltd. profitiert wirtschaftlich erheblich von den erbrachten Dienstleistungen. Anxun Information Technology Co. Ltd. ist daher für Cyberangriffe mit erheblichen Auswirkungen verantwortlich, die eine äußere Bedrohung für die Mitgliedstaaten darstellen, sowie für Angriffe auf Drittstaaten. Wu Haibo war an der Steuerung versuchter Cyberangriffe mit erheblichen Auswirkungen auf Mitgliedstaaten und an der Ermutigung dazu beteiligt. In dieser Funktion ist er für Cyberangriffe mit erheblichen Auswirkungen, die eine äußere Bedrohung für die Mitgliedstaaten darstellen, sowie für Cyberangriffe mit erheblichen Auswirkungen auf Drittstaaten verantwortlich und an diesen beteiligt.	16.3.2026“

2. Folgende Einträge werden unter der Überschrift „B. Juristische Personen, Organisationen und Einrichtungen“ angefügt:

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
„5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (chinesische Schreibweise) Aliasname: Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited Adresse: Fenghao East Road, Room 103, Building 6, No. 9, Beijing Haidian District, China Ort der Registrierung: Peking, China Registrierungsdatum: 2.9.2010 Unified Social Credit Code (Chinesische Steuernummer): 91110108562135265P	Integrity Technology Group ist ein in der Volksrepublik China ansässiges Cybersicherheitsunternehmen, das Cyberangriffe erleichtert hat, die mit ‚Advanced Persistent Threat (APT) Flax Typhoon‘, in Verbindung gebracht werden. Diese Gruppe hat die Produkte und Technologien von Integrity Technology Group für seine Aktivitäten der Computer-Netzwerk-Ausnutzung (Computer Network Exploitation, CNE) verwendet. Die Produkte von Integrity Technology Group werden seither genutzt, um Geräte des Internets der Dinge in den Mitgliedstaaten, sowie in Ländern in ganz Europa und weltweit zu kompromittieren und auf diese zuzugreifen. Zwischen 2022 und 2023 hat Flax Typhoon unter Verwendung der Produkte von Integrity Technology Group auf mindestens 65 600 Geräte des Internets der Dinge in sechs Mitgliedstaaten zugegriffen. Daher wurden die kommerziellen Produkte und die kommerzielle Infrastruktur von Integrity Technology Group regelmäßig bei Cyberangriffen auf Mitgliedstaaten und Drittstaaten eingesetzt. Folglich leistet die Integrity Technology Group durch die Beeinträchtigungen von Informationssystemen im Zusammenhang mit digitaler Infrastruktur technische und materielle Unterstützung für Cyberangriffe mit erheblichen Auswirkungen, die eine äußere Bedrohung für Mitgliedstaaten und Drittstaaten darstellen.	16.3.2026

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
6.	Emennet Pasargad	Aliasname: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten Ort der Registrierung: Teheran, Iran Registrierungsnummer: 554267 Ort des Hauptgeschäftssitzes: Teheran, Iran	Emennet Pasargad ist ein iranischer Cyberakteur (Unternehmen), der zahlreiche Einrichtungen, insbesondere in den Mitgliedstaaten und in den Vereinigten Staaten (USA), angegriffen hat. Unter dem Aliasnamen ‚Anzu Team' hat Emennet Pasargad digitale Infrastruktur in Schweden angegriffen und einen schwedischen SMS-Dienst kompromittiert, mit Folgen für eine große Zahl von Personen. Darüber hinaus hat die Organisation unter dem Aliasnamen ‚Holy Souls' die Abonnentendatenbank der französischen Satirezeitschrift Charlie Hebdo kompromittiert und diese im Dark Web zum Verkauf angeboten. Emennet Pasargad kompromittierte während der Olympischen Spiele in Paris Werbetafeln und zeigte Desinformationskampagnen. Emennet Pasargad versuchte auch, Einfluss auf die US-Präsidentschaftswahlen von 2020 zu nehmen und damit die Demokratie und die Rechtsstaatlichkeit zu bedrohen, indem es sich Zugriff auf vertrauliche Wählerinformationen aus den USA verschaffte und unbefugt Zugang zum Computernetzwerk eines US-Medienunternehmens erlangte. Emennet Pasargad ist daher für Cyberangriffe mit erheblichen Auswirkungen, die eine äußere Bedrohung für die Mitgliedstaaten darstellen, und für Cyberangriffe mit erheblichen Auswirkungen auf einen Drittstaat verantwortlich.	16.3.2026

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
7.	Anxun Information Technology Co. Ltd.	安洵信息技术有限公司 (chinesische Schreibweise) Aliasname: i-Soon Adresse: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai Unified Social Credit Code (Chinesische Steuernummer): 91510105332025597A (Zweigniederlassung Sichuan) Unified Social Credit Code (Chinesische Steuernummer): 91310116561906136G (Zweigniederlassung Shanghai) Website: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win Telefonnummern: +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. ist ein in der Volksrepublik China (VR China) ansässiges Unternehmen, das ‚Hack-for-hire'-Dienstleistungen anbietet. Es hat gezielt kritische Infrastrukturen und kritische staatliche Funktionen der Mitgliedstaaten angegriffen sowie auf Verschlusssachen zugegriffen und diese verkauft. Darüber hinaus hat Anxun Information Technology Co. Ltd. die Regierungen verschiedener Drittstaaten angegriffen und damit eine Bedrohung für die Ziele der Gemeinsamen Außen- und Sicherheitspolitik (GASP) der Union gemäß Artikel 21 Absatz 2 Buchstaben a bis c des Vertrags über die Europäische Union dargestellt. Anxun Information Technology Co. Ltd. profitiert wirtschaftlich erheblich von den erbrachten Dienstleistungen. Anxun Information Technology Co. Ltd. ist daher für Cyberangriffe mit erheblichen Auswirkungen, die eine äußere Bedrohung für die Mitgliedstaaten darstellen, sowie für Cyberangriffe mit erheblichen Auswirkungen auf Drittstaaten verantwortlich.	16.3.2026“