2026/1078

12.5.2026

DURCHFÜHRUNGSVERORDNUNG (EU) 2026/1078 DES RATES

vom 11. Mai 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,

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) Der Rat hat die in Anhang I der Verordnung (EU) 2019/796 enthaltene Liste der natürlichen und juristischen Personen, Organisationen und Einrichtungen überprüft. Auf der Grundlage dieser Überprüfung sollten die Gründe für die Aufnahme von vier Personen und einer Organisation in die Liste der natürlichen und juristischen Personen, Organisationen und Einrichtungen, die restriktiven Maßnahmen unterliegen, aktualisiert werden.

(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 nach 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 11. Mai 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. Die Einträge 1, 2, 13 und 14 unter der Überschrift „A. Natürliche Personen“ erhalten folgende Fassung:

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
„1.	GAO Qiang	Geburtsdatum: 4. Oktober 1983 Geburtsort: Provinz Shandong, China Anschrift: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Staatsangehörigkeit: chinesisch Geschlecht: männlich	Gao Qiang wird mit der Dachorganisation ‚APT10‘ (‚Advanced Persistent Threat 10‘) (alias ‚Red Apollo‘, ‚CVNX‘, ‚Stone Panda‘, ‚MenuPass‘ und ‚Potassium‘) in Verbindung gebracht und war an der ‚Operation Cloud Hopper‘, einer Reihe von Cyberangriffen mit erheblichen Auswirkungen, die von außerhalb der Union verübt werden und eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen, und von Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten, beteiligt. Mit der ‚Operation Cloud Hopper‘ wurden Informationssysteme multinationaler Unternehmen auf sechs Kontinenten angegriffen, darunter Unternehmen mit Sitz in der Union, und es wurde unbefugt auf sensible Geschäftsdaten zugegriffen, was zu erheblichen wirtschaftlichen Verlusten geführt hat. Gao Qiang wird mit der Führungs- und Kontrollinfrastruktur von APT10 in Verbindung gebracht. Überdies ist er bei Huaying Haitai beschäftigt, einer Organisation, die von APT10 genutzt wird und die benannt wurde, weil sie ‚Operation Cloud Hopper‘ unterstützt und erleichtert. Er steht ferner in Verbindung mit Zhang Shilong, der mit APT10 in Verbindung gebracht wird und der auch bei Huaying Haitai beschäftigt ist.	30.7.2020

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
2.	ZHANG Shilong	Geburtsdatum: 10. September 1981 Geburtsort: China Anschrift: Anschrift: Hedong, Yuyang Road No 121, Tianjin, China Staatsangehörigkeit: chinesisch Geschlecht: männlich	Zhang Shilong wird der Dachorganisation ‚APT10' (‚Advanced Persistent Threat 10') (alias ‚Red Apollo', ‚CVNX', ‚Stone Panda', ‚MenuPass' und ‚Potassium') in Verbindung gebracht und war an der ‚Operation Cloud Hopper', einer Reihe von Cyberangriffen mit erheblichen Auswirkungen, die von außerhalb der Union verübt werden und eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen, und von Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten, beteiligt. Mit der ‚Operation Cloud Hopper' wurden Informationssysteme multinationaler Unternehmen auf sechs Kontinenten angegriffen, darunter Unternehmen mit Sitz in der Union, und es wurde unbefugt auf sensible Geschäftsdaten zugegriffen, was zu erheblichen wirtschaftlichen Verlusten geführt hat. Zhang Shilong wird unter anderem über die Schadsoftware, die er im Zusammenhang mit den Cyberangriffen von APT10 entwickelt und getestet hat, mit APT10 in Verbindung gebracht. Überdies ist Zhang Shilong bei Huaying Haitai beschäftigt, einer Organisation, die von APT10 genutzt wird und die benannt wurde, weil sie ‚Operation Cloud Hopper' unterstützt und erleichtert. Er steht ferner in Verbindung mit Gao Qiang, der mit APT10 in Verbindung gebracht wird und der auch bei Huaying Haitai beschäftigt ist.	30.7.2020

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Geburtsdatum: 20.4.1989 Geburtsort: Serpukhov, Russische Föderation Staatsangehörigkeit: russisch Anschrift: Serpukhov Geschlecht: männlich	Mikhail Mikhailovich Tsarev war an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Mitgliedstaaten der EU darstellen. Mikhail Mikhailovich Tsarev, auch bekannt unter den Online-Spitznamen ‚Mango', ‚Alexander Grachev', ‚Super Misha', ‚Ivanov Mixail', ‚Misha Krutysha' und ‚Nikita Andreevich Tsarev', ist ein wichtiger Akteur in der Einsetzung der Schadsoftware ‚Conti' und ‚Trickbot' und ist an der Russland-basierten Bedrohungsgruppe ‚Wizard Spider' beteiligt. Wizard Spider entwickelt sich ständig weiter und intensiviert seine Operationen. Die Schadsoftwares ‚Conti' und ‚Trickbot' wurden von ‚Wizard Spider' geschaffen und entwickelt. ‚Wizard Spider' hat in verschiedenen Branchen, darunter wesentliche Dienstleistungsbereiche wie die Gesundheitsversorgung und das Bankwesen, Ransomware-Kampagnen durchgeführt. Die Gruppe hat weltweit Computer infiziert und ihre Schadsoftware zu einer hochmodularen Schadsoftware-Reihe entwickelt. Von der Gruppe ‚Wizard Spider' durchgeführte Kampagnen, bei denen Schadsoftware wie ‚Conti', ‚Ryuk', ‚TrickBot' oder ‚Black Basta' eingesetzt wird, sind für erhebliche wirtschaftliche Schäden in der Europäischen Union verantwortlich. Deshalb ist Mikhail Mikhailovich Tsarev an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.	24.6.2024

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
14.	Maksim Sergeevich GALOCHKIN	Максим Сергеевич ГАЛОЧКИН Geburtsdatum: 19.5.1982 Geburtsort: Abakan, Russische Föderation Staatsangehörigkeit: russisch Geschlecht: männlich	Maksim Galochkin hat an Cyberangriffen mit erheblichen Auswirkungen mitgewirkt, die eine externe Bedrohung für die Mitgliedstaaten der EU darstellen. Maksim Galochkin ist auch bekannt unter den Online-Spitznamen ‚Benalen', ‚Bentley', ‚Volhvb', ‚volhvb', ‚manuel', ‚Max17' und ‚Crypt'. Galochkin ist ein wichtiger Akteur bei der Einsetzung der Schadsoftware ‚TrickBot' und ‚Conti' und ist an der Russland-basierten Bedrohungsgruppe ‚Wizard Spider' beteiligt. Er hat ein Team von Testern geleitet, das für die Entwicklung, Überwachung und Durchführung von Tests für die von ‚Wizard Spider' geschaffene und eingesetzte TrickBot-Schadsoftware verantwortlich war. Wizard Spider entwickelt sich ständig weiter und intensiviert seine Aktivitäten. ‚Wizard Spider' hat in verschiedenen Branchen, darunter wesentliche Dienstleistungsbereiche wie die Gesundheitsversorgung und das Bankwesen, Ransomware-Kampagnen durchgeführt. Die Gruppe hat weltweit Computer infiziert und ihre Schadsoftware in eine hochmodulare Schadsoftware-Reihe entwickelt. Von der Gruppe ‚Wizard Spider' durchgeführte Kampagnen, bei denen Schadsoftware wie ‚Conti', ‚Ryuk', ‚TrickBot' oder ‚Black Basta' eingesetzt wird, sind für erhebliche wirtschaftliche Schäden in der Europäischen Union verantwortlich. Deshalb ist Maksim Galochkin an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.	24.6.2024“

2. Der Eintrag 1 unter der Überschrift „B. Juristische Personen, Organisationen und Einrichtungen“ erhält folgende Fassung:

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
„1.	Tianjin Huaying Haitai Science and Technology Development Co Ltd (Huaying Haitai)	Aliasname: Haitai Technology Development Co. Ltd Ort: Tianjin, China	Die Huaying Haitai hat die ‚Operation Cloud Hopper‘ finanziell, technisch oder materiell unterstützt; es handelt sich dabei um eine Reihe von Cyberangriffen mit erheblichen Auswirkungen, die von außerhalb der Union ausgehen und eine externe Bedrohung für die Union bzw. ihre Mitgliedstaaten darstellen und von Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten. Mit der ‚Operation Cloud Hopper‘ wurden Informationssysteme multinationaler Unternehmen auf sechs Kontinenten angegriffen, darunter Unternehmen mit Sitz in der Union, und unbefugt auf sensible Geschäftsdaten zugegriffen, was zu erheblichen wirtschaftlichen Verlusten geführt hat. Die ‚Operation Cloud Hopper‘ wurde von dem als ‚APT10‘ (‚Advanced Persistent Threat 10‘) (alias ‚Red Apollo‘, ‚CVNX‘, ‚Stone Panda‘, ‚MenuPass‘ und ‚Potassium‘) bekannten Täter verübt. Die Huaying Haitai kann mit APT10 in Verbindung gebracht werden. Darüber hinaus waren Gao Qiang und Zhang Shilong bei Huaying Haitai beschäftigt, die beide in Zusammenhang mit der ‚Operation Cloud Hopper‘ gebracht werden. Die Huaying Haitai steht daher ebenfalls in Beziehung zu Gao Qiang und Zhang Shilong.	30.7.2020“