Amtsblatt
der Europäischen Union

DE
Reihe L

2024/1778

24.6.2024

DURCHFÜHRUNGSVERORDNUNG (EU) 2024/1778 DES RATES

vom 24. Juni 2024

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 des Hohen Vertreters 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) Gezielte restriktive Maßnahmen gegen Cyberangriffe mit erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen, gehören zu den Maßnahmen des Rahmens für eine gemeinsame diplomatische Reaktion der Union auf böswillige Cyberaktivitäten („Cyber Diplomacy Toolbox“) und sind ein wichtiges Instrument, um solche Aktivitäten zu verhindern, von solchen Aktivitäten abzuschrecken, davon abzuhalten und darauf zu reagieren.

(3) Böswillige Cyberaktivitäten, die gegen kritische Infrastruktur oder wesentliche Dienstleistungen gerichtet sind und zu denen unter anderem der Einsatz von Ransomware und Wiper-Schadsoftware gehört, die gezielte Ausrichtung gegen Lieferketten und Cyberspionage, einschließlich des Diebstahls geistigen Eigentums, nehmen an Zahl, Häufigkeit und Komplexität zu. Durch ihre beeinträchtigenden und zerstörerischen Auswirkungen stellen diese Aktivitäten eine systemische Bedrohung für die Sicherheit, die Wirtschaft, die Demokratie und die Gesellschaft der Union insgesamt dar.

(4) Der Einsatz von Cyberoperationen, die den grundlosen und ungerechtfertigten Angriffskrieg Russlands gegen die Ukraine ermöglichen und damit einhergehen, beeinträchtigt die globale Stabilität und Sicherheit, stellt ein erhebliches Eskalationsrisiko dar und erhöht den bereits in den letzten Jahren verzeichneten deutlichen Anstieg böswilliger Cyberaktivitäten außerhalb des bewaffneten Konflikts. Angesichts der zunehmenden Cybersicherheitsrisiken und der insgesamt komplexen Cyberbedrohungslandschaft, in der eindeutig die Gefahr eines raschen Übergreifens von Cybervorfällen von einem Mitgliedstaat auf andere Mitgliedstaaten und von Drittländern auf die Union besteht, sind weitere restriktive Maßnahmen im Rahmen der Verordnung (EU) 2019/796 erforderlich.

(5) Als Teil dauerhafter, maßgeschneiderter und koordinierter Maßnahmen der Union gegen Akteure, von denen eine anhaltende Cyberbedrohung ausgeht, sollten sechs natürliche Personen in die Liste der natürlichen und juristischen Personen, Organisationen und Einrichtungen, die restriktiven Maßnahmen unterliegen, in Anhang I der Verordnung (EU) 2019/796 aufgenommen werden. Diese Personen sind für Cyberangriffe mit erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen, verantwortlich oder waren an solchen Angriffen beteiligt.

(6) 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 nach Maßgabe des Anhangs der vorliegenden Verordnung geändert.

([1]) ABl. L 129 I vom 17.5.2019, S. 1.

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 Luxemburg am 24. Juni 2024.

Im Namen des Rates

Der Präsident

J. BORRELL FONTELLES

ANHANG

In Anhang I der Verordnung (EU) 2019/796 werden dem Abschnitt „A. Natürliche Personen“ folgende Einträge angefügt:

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
„9.	Ruslan Aleksandrovich PERETYATKO	Руслан Александрович ПЕРЕТЯТЬКО Geburtsdatum: 3.8.1985 Staatsangehörigkeit: russisch Geschlecht: männlich	Ruslan PERETYATKO war an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen. Ruslan PERETYATKO gehört der ‚Callisto‘-Gruppe an, einer Gruppe von Beamten des russischen Militärgeheimdienstes, die Cyberoperationen gegen Mitgliedstaaten der EU und Drittstaaten durchführt. Die ‚Callisto‘-Gruppe (alias ‚Seaborgium‘, ‚Star Blizzard‘„ColdRiver‘, ‚TA446‘) hat mehrjährige Phishing-Kampagnen gestartet, um Kontozugangsdaten und Daten zu stehlen. Darüber hinaus zeichnet die ‚Callisto‘-Gruppe für Kampagnen verantwortlich, die sich gegen Einzelpersonen und kritische staatliche Funktionen, auch in den Bereichen Verteidigung und Außenbeziehungen, richten. Deshalb ist Ruslan PERETYATKO an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.	24.6.2024
10.	Andrey Stanislavovich KORINETS	Андрей Станиславович КОРИНЕЦ Geburtsdatum: 18.5.1987 Geburtsort: Stadt Syktyvkar, Russland Staatsangehörigkeit: russisch Geschlecht: männlich	Andrey Stanislavovich KORINETS war an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen. Andrey Stanislavovich KORINETS ist Offizier des ‚Center 18‘ des Inlandsgeheimdienstes der Russischen Föderation. Andrey Stanislavovich KORINETS gehört der ‚Callisto-Gruppe‘ an, einer Gruppe von Beamten des russischen Militärgeheimdienstes, die Cyberoperationen gegen Mitgliedstaaten der EU und Drittstaaten durchführt. Die ‚Callisto‘-Gruppe (alias ‚Seaborgium‘, ‚Star Blizzard‘„ColdRiver‘, ‚TA446‘) hat mehrjährige Phishing-Kampagnen gestartet, um Kontozugangsdaten und Daten zu stehlen. Darüber hinaus zeichnet die ‚Callisto‘-Gruppe für Kampagnen verantwortlich, die sich gegen Einzelpersonen und kritische staatliche Funktionen, auch in den Bereichen Verteidigung und Außenbeziehungen, richten. Deshalb ist Andrey Stanislavovich KORINETS 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
11.	Oleksandr SKLIANKO	Александр СКЛЯНКО (russische Schreibweise) Олександр СКЛЯНКО (ukrainische Schreibweise) Geburtsdatum: 5.8.1973 Reisepass: EC 867868, ausgestellt am 27.11.1998 (Ukraine) Geschlecht: männlich	Oleksandr SKLIANKO war an Cyberangriffen mit erheblichen Auswirkungen, die gegen Mitgliedstaaten der EU gerichtet waren, sowie an Cyberangriffen mit erheblichen Auswirkungen, die gegen Drittstaaten gerichtet waren, beteiligt. Oleksandr SKLIANKO gehört der ‚Armageddon'-Hackergruppe an, die vom Inlandsgeheimdienst der Russischen Föderation unterstützt wird und verschiedene Cyberangriffe mit erheblichen Auswirkungen durchgeführt hat, die gegen die Regierung der Ukraine und gegen Mitgliedstaaten der EU und deren Regierungsbeamte gerichtet waren, unter anderem mittels Phishing-E-Mails und Schadsoftware-Kampagnen. Deshalb ist Oleksandr SKLIANKO an Cyberangriffen mit erheblichen Auswirkungen, die gegen Drittstaaten gerichtet sind, sowie an Cyberangriffen mit erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen, beteiligt.	24.6.2024
12.	Mykola CHERNYKH	Николай ЧЕРНЫХ (russische Schreibweise) Микола ЧЕРНИХ (ukrainische Schreibweise) Geburtsdatum: 12.10.1978 Reisepass: EC 922162, ausgestellt am 20.1.1999 (Ukraine) Geschlecht: männlich	Mykola CHERNYKH war an Cyberangriffen mit erheblichen Auswirkungen, die gegen Mitgliedstaaten der EU gerichtet waren, sowie an Cyberangriffen mit erheblichen Auswirkungen, die gegen Drittstaaten gerichtet waren, beteiligt. Mykola CHERNYKH gehört der ‚Armageddon'-Hackergruppe an, die vom Inlandsgeheimdienst der Russischen Föderation unterstützt wird und verschiedene Cyberangriffe mit erheblichen Auswirkungen durchgeführt hat, die gegen die Regierung der Ukraine und gegen Mitgliedstaaten der EU und deren Regierungsbeamte gerichtet waren, unter anderem mittels Phishing-E-Mails und Schadsoftware-Kampagnen. Als ehemaliger Mitarbeiter des Sicherheitsdienstes der Ukraine ist er in der Ukraine des Verrats und des unberechtigten Eingriffs in den Betrieb elektronischer Rechner und automatisierter Systeme angeklagt. Deshalb ist Mykola CHERNYKH 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
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. Die Schadsoftware ‚Conti' und ‚Trickbot' wurde von ‚Wizard Spider' geschaffen und entwickelt wurde. Die Gruppe ‚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' und ‚TrickBot', 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 bei 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 in 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 mit für die Entwicklung, Überwachung und Durchführung von Tests für die von ‚Wizard Spider' geschaffene und eingesetzte TrickBot-Schadsoftware verantwortlich war. ‚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' und ‚TrickBot', 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“