2024/1391

17.5.2024

BESCHLUSS (GASP) 2024/1391 DES RATES

vom 17. Mai 2024

zur Änderung des Beschlusses (GASP) 2019/797 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen

DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Europäische Union, insbesondere auf Artikel 29,

auf Vorschlag des Hohen Vertreters der Union für Außen- und Sicherheitspolitik,

in Erwägung nachstehender Gründe:

(1) Der Rat hat am 17. Mai 2019 den Beschluss (GASP) 2019/797 ([1]) angenommen.

(2) Der Beschluss (GASP) 2019/797 gilt bis zum 18. Mai 2025. Aufgrund einer Überprüfung des genannten Beschlusses sollten die darin festgelegten restriktiven Maßnahmen bis zu diesem Zeitpunkt verlängert werden.

(3) Angesichts der fortgesetzten und zunehmenden böswilligen Handlungen im Cyberraum, einschließlich gegen Drittstaaten gerichteter Handlungen, sollten die Gründe für die Aufnahme von sechs Personen und zwei Organisationen in die Liste der natürlichen und juristischen Personen, Organisationen und Einrichtungen, die den im Anhang des Beschlusses (GASP) 2019/797 festgelegten restriktiven Maßnahmen unterliegen, aktualisiert werden.

(4) Der Beschluss (GASP) 2019/797 sollte daher entsprechend geändert werden —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Der Beschluss (GASP) 2019/797 wird wie folgt geändert:

1. Artikel 10 erhält folgende Fassung:

   „*Artikel 10*

   Dieser Beschluss gilt bis zum 18. Mai 2025 und wird fortlaufend überprüft.“

2. Der Anhang wird gemäß dem Anhang des vorliegenden Beschlusses geändert.

Artikel 2

Dieser Beschluss tritt am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Geschehen zu Brüssel am 17. Mai 2024.

Im Namen des Rates

Die Präsidentin

H. LAHBIB

([1]) Beschluss (GASP) 2019/797 des Rates vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen (ABl. L 129 I vom 17.5.2019, S. 13).

ANHANG

Der Anhang des Beschlusses (GASP) 2019/797 („Liste der natürlichen und juristischen Personen, Organisationen und Einrichtungen gemäß den Artikeln 4 und 5“) wird wie folgt geändert:

1. In der Liste mit der Überschrift „A. Natürliche Personen“ erhalten die Einträge 3 bis 8 folgende Fassung:

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
„3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Geburtsdatum: 27.5.1972 Geburtsort: Oblast Perm, Russische SFSR (jetzt Russische Föderation) Reisepass-Nr.: 120017582 ausgestellt vom Außenministerium der Russischen Föderation gültig vom 17.4.2017 bis zum 17.4.2022 Ort: Moskau, Russische Föderation Staatsangehörigkeit: russisch Geschlecht: männlich	Alexey Minin hat an einem versuchten Cyberangriff auf die Organisation für das Verbot chemischer Waffen (OVCW) in den Niederlanden mit potenziell erheblichen Auswirkungen sowie an Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten teilgenommen. Als für ‚human intelligence‘ (Aufklärung mit menschlichen Quellen) zuständiger Mitarbeiter der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU) gehörte Alexey Minin einem Team von vier Beamten des russischen Militärgeheimdienstes an, die im April 2018 versuchten, sich unbefugt Zugang zum WiFi-Netz der OVCW in Den Haag (Niederlande) zu verschaffen. Der versuchte Cyberangriff hatte zum Ziel, in das WiFi-Netz der OVCW einzudringen, was bei Erfolg die Sicherheit des Netzes und die laufenden Untersuchungen der OVCW gefährdet hätte. Der niederländische militärische Nachrichten- und Sicherheitsdienst (Militaire Inlichtingen- en Veiligheidsdienst) hat den versuchten Cyberangriff abgewehrt und damit die OVCW vor einem schweren Schaden bewahrt. Eine Grand Jury des Western District of Pennsylvania (Vereinigte Staaten von Amerika) hat Alexey Minin als Beamter der Hauptdirektion des russischen Militärgeheimdienstes (GRU) wegen Computerhackings, Telekommunikationsbetrugs, schweren Identitätsdiebstahls und Geldwäsche angeklagt.	30.7.2020

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Geburtsdatum: 31.7.1977 Geburtsort: Oblast Murmansk, Russische SFSR (jetzt Russische Föderation) Reisepass-Nr.: 100135556 ausgestellt vom Außenministerium der Russischen Föderation gültig vom 17.4.2017 bis zum 17.4.2022 Ort: Moskau, Russische Föderation Staatsangehörigkeit: russisch Geschlecht: männlich	Aleksei Morenets hat an einem versuchten Cyberangriff auf die Organisation für das Verbot chemischer Waffen (OVCW) in den Niederlanden mit potenziell erheblichen Auswirkungen sowie an Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten teilgenommen. Als Cyber-Operator der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU) gehörte Aleksei Morenets einem Team von vier Beamten des russischen Militärgeheimdienstes an, die im April 2018 versuchten, sich unbefugt Zugang zum WiFi-Netz der OVCW in Den Haag (Niederlande) zu verschaffen. Der versuchte Cyberangriff hatte zum Ziel, in das WiFi-Netz der OVCW einzudringen, was bei Erfolg die Sicherheit des Netzes und die laufenden Untersuchungen der OVCW gefährdet hätte. Der niederländische militärische Nachrichten- und Sicherheitsdienst (Militaire Inlichtingen- en Veiligheidsdienst) hat den versuchten Cyberangriff abgewehrt und damit die OVCW vor einem schweren Schaden bewahrt. Eine Grand Jury des Western District of Pennsylvania (Vereinigte Staaten von Amerika) hat Aleksei Morenets, der der Militäreinheit 26165 zugewiesen ist, wegen Computerhackings, Telekommunikationsbetrugs, schweren Identitätsdiebstahls und Geldwäsche angeklagt.	30.7.2020

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Geburtsdatum: 26.7.1981 Geburtsort: Kursk, Russische SFSR (jetzt Russische Föderation) Reisepass-Nr.: 100135555 ausgestellt vom Außenministerium der Russischen Föderation gültig vom 17.4.2017 bis zum 17.4.2022 Ort: Moskau, Russische Föderation Staatsangehörigkeit: russisch Geschlecht: männlich	Evgenii Serebriakov hat an einem versuchten Cyberangriff auf die Organisation für das Verbot chemischer Waffen (OVCW) in den Niederlanden mit potenziell erheblichen Auswirkungen sowie an Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten teilgenommen. Als Cyber-Operator der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU) gehörte Evgenii Serebriakov einem Team von vier Beamten des russischen Militärgeheimdienstes an, die im April 2018 versuchten, sich unbefugt Zugang zum WiFi-Netz der OVCW in Den Haag (Niederlande) zu verschaffen. Der versuchte Cyberangriff hatte zum Ziel, in das WiFi-Netz der OVCW einzudringen, was bei Erfolg die Sicherheit des Netzes und die laufenden Untersuchungen der OVCW gefährdet hätte. Der niederländische militärische Nachrichten- und Sicherheitsdienst (Militaire Inlichtingen- en Veiligheidsdienst) hat den versuchten Cyberangriff abgewehrt und damit die OVCW vor einem schweren Schaden bewahrt. Seit Frühjahr 2022 ist Evgenii Serebriakov Anführer von ‚Sandworm' (alias ‚Sandworm Team', ‚BlackEnergy Group', ‚Voodoo Bear', ‚Quedagh', ‚Olympic Destroyer' und ‚Telebots'), einer Täter- und Hackergruppe, die mit der Einheit 74455 der Hauptdirektion des russischen Militärgeheimdienstes in Verbindung steht. Sandworm hat im Zuge des Angriffskriegs Russlands gegen die Ukraine Cyberangriffe auf die Ukraine, einschließlich auf ukrainische Regierungsstellen, verübt.	30.7.2020

ELI: http://data.europa.eu/eli/dec/2024/1391/oj
ABl. L vom 17.5.2024

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Geburtsdatum: 24.8.1972 Geburtsort: Uljanowsk, Russische SFSR (jetzt Russische Föderation) Reisepass-Nr.: 120018866 ausgestellt vom Außenministerium der Russischen Föderation gültig vom 17.4.2017 bis zum 17.4.2022 Ort: Moskau, Russische Föderation Staatsangehörigkeit: russisch Geschlecht: männlich	Oleg Sotnikov hat an einem versuchten Cyberangriff auf die Organisation für das Verbot chemischer Waffen (OVCW) in den Niederlanden mit potenziell erheblichen Auswirkungen sowie an Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten teilgenommen. Als für ‚human intelligence' (Aufklärung mit menschlichen Quellen) zuständiger Mitarbeiter der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU) gehörte Oleg Sotnikov einem Team von vier Beamten des russischen Militärgeheimdienstes an, die im April 2018 versuchten, sich unbefugt Zugang zum WiFi-Netz der OVCW in Den Haag (Niederlande) zu verschaffen. Der versuchte Cyberangriff hatte zum Ziel, in das WiFi-Netz der OVCW einzudringen, was bei Erfolg die Sicherheit des Netzes und die laufenden Untersuchungen der OVCW gefährdet hätte. Der niederländische militärische Nachrichten- und Sicherheitsdienst (Militaire Inlichtingen- en Veiligheidsdienst) hat den versuchten Cyberangriff abgewehrt und damit die OVCW vor einem schweren Schaden bewahrt. Eine Grand Jury des Western District of Pennsylvania hat Oleg Sotnikov als Beamter der Hauptdirektion des russischen Militärgeheimdienstes (GRU) wegen Computerhackings, Telekommunikationsbetrugs, schweren Identitätsdiebstahls und Geldwäsche angeklagt.	30.7.2020

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Geburtsdatum: 15.11.1990 Geburtsort: Kursk, Russische SFSR (jetzt Russische Föderation) Staatsangehörigkeit: russisch Geschlecht: männlich	Dmitry Badin war an einem Cyberangriff mit erheblichen Auswirkungen gegen den Deutschen Bundestag sowie an Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten beteiligt. Als Militärgeheimdienstbeamter des 85. Hauptzentrums für Spezialdienste (GTsST) der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU) war Dmitry Badin Teil eines Teams von Beamten des russischen Militärgeheimdienstes, die im April und Mai 2015 einen Cyberangriff gegen den Deutschen Bundestag durchführten. Dieser Cyberangriff zielte auf das Informationssystem des Parlaments ab und beeinträchtigte dessen Betrieb für mehrere Tage. Es wurde eine beträchtliche Menge an Daten gestohlen, und die E-Mail-Konten mehrerer MdB sowie der ehemaligen Bundeskanzlerin Angela Merkel waren betroffen. Eine Grand Jury des Western District of Pennsylvania (Vereinigte Staaten von Amerika) hat Dmitry Badin, der der Militäreinheit 26165 zugewiesen ist, wegen Computerhackings, Telekommunikationsbetrugs, schweren Identitätsdiebstahls und Geldwäsche angeklagt.	22.10.2020

ELI: http://data.europa.eu/eli/dec/2024/1391/oj

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Geburtsdatum: 21.2.1961 Staatsangehörigkeit: russisch Geschlecht: männlich	Igor Kostyukov ist derzeit Leiter der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU), wo er zuvor als Erster Stellvertretender Leiter tätig war. Eine der seiner Befehlsgewalt unterstehenden Einheiten ist das 85. Hauptzentrum für Spezialdienste (GTsST), (alias ‚Militäreinheit 26165', ‚APT28', ‚Fancy Bear', ‚Sofacy Group', ‚Pawn Storm' und ‚Strontium'). In dieser Eigenschaft ist Igor Kostyukov verantwortlich für vom GTsST durchgeführte Cyberangriffe, einschließlich derjenigen mit erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen. Militärgeheimdienstbeamte des GTsST waren insbesondere beteiligt am Cyberangriff gegen den Deutschen Bundestag im April und Mai 2015, und an dem versuchten Cyberangriff vom April 2018 in den Niederlanden mit dem Ziel, sich unbefugt Zugang zum WiFi-Netz der Organisation für das Verbot chemischer Waffen (OVCW) zu verschaffen. Der Cyberangriff gegen den Deutschen Bundestag zielte auf das Informationssystem des Parlaments ab und beeinträchtigte dessen Betrieb für mehrere Tage. Es wurde eine beträchtliche Menge an Daten gestohlen, und die E-Mail-Konten mehrerer MdB sowie der ehemaligen Bundeskanzlerin Angela Merkel waren betroffen.	22.10.2020“

2. In der Liste mit der Überschrift „B. Juristische Personen, Organisationen und Einrichtungen“ erhalten die Einträge 3 und 4 folgende Fassung:

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
„3	Hauptzentrum für Spezialtechnologien (GTsST) der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU)	Adresse: 22 Kirova Street, Moscow, Russian Federation	Das Hauptzentrum für Spezialtechnologien (GTsST) der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU), auch unter seiner Feldpostnummer 74455 bekannt, ist an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die von außerhalb der Union ausgehen und eine externe Bedrohung für die Union bzw. ihre Mitgliedstaaten darstellen, und an Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten; dazu zählen die als ‚NotPetya‘ oder ‚EternalPetya‘ bekannten Cyberangriffe vom Juni 2017 und die im Winter 2015 und 2016 gegen das ukrainische Stromnetz gerichteten Cyberangriffe. ‚NotPetya‘ und ‚EternalPetya‘ haben in einer Reihe von Unternehmen in der Union, in Europa außerhalb der Union und auf der ganzen Welt Daten unzugänglich gemacht, indem Ransomware in Computer eingeschleust und der Zugriff auf Daten blockiert wurde, was u. a. zu erheblichen wirtschaftlichen Verlusten geführt hat. Der Cyberanschlag auf ein ukrainisches Stromnetz hat dazu geführt, dass Teile des Netzes im Winter abgeschaltet wurden. ‚NotPetya‘ und ‚EternalPetya‘ wurden von dem als ‚Sandworm‘ (alias ‚Sandworm Team‘, ‚BlackEnergy Group‘, ‚Voodoo Bear‘, ‚Quedagh‘, ‚Olympic Destroyer‘ und ‚Telebots‘) bekannten Täter verübt, der auch den Angriff auf das ukrainische Stromnetz ausgeführt hat. Sandworm hat im Zuge des Angriffskriegs Russlands gegen die Ukraine Cyberangriffe auf die Ukraine, einschließlich auf Regierungsstellen und kritische Infrastruktur der Ukraine, verübt. Zu diesen Cyberangriffen gehören Spear-Phishing-Kampagnen und Angriffe mit Schadsoftware und Ransomware. Das Hauptzentrum für Spezialtechnologien der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation spielt eine aktive Rolle bei den Cyberaktivitäten von ‚Sandworm‘ und kann mit ‚Sandworm‘ in Verbindung gebracht werden.	30.7.2020

ELI: http://data.europa.eu/eli/dec/2024/1391/oj

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
4.	85. Hauptzentrum für Spezialdienste (GTsST) der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU)	Adresse: Komsomol'skiy Prospekt, 20, Moskau, 119146, Russische Föderation	Das 85. Hauptzentrum für Spezialdienste (GTsST) der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GU/GRU), (alias ‚Militäreinheit 26165', ‚APT28', ‚Fancy Bear', ‚Sofacy Group', ‚Pawn Storm' und ‚Strontium'), ist an Cyberangriffen mit erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen, sowie an Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten beteiligt. Militärgeheimdienstbeamte des GTsST waren insbesondere beteiligt am Cyberangriff gegen den Deutschen Bundestag im April und Mai 2015, und an dem versuchten Cyberangriff vom April 2018 in den Niederlanden mit dem Ziel, sich unbefugt Zugang zum WiFi-Netz der Organisation für das Verbot chemischer Waffen (OVCW) zu verschaffen. Der Cyberangriff gegen den Deutschen Bundestag zielte auf das Informationssystem des Parlaments ab und beeinträchtigte dessen Betrieb für mehrere Tage. Es wurde eine beträchtliche Menge an Daten gestohlen, und die E-Mail-Konten mehrerer MdB sowie der ehemaligen Bundeskanzlerin Angela Merkel waren betroffen. Im Zuge des Angriffskrieg Russlands gegen die Ukraine wurden durch das GTsST Cyberangriffe (Spear-Phishing-Angriffe und Angriffe mit Schadsoftware) gegen die Ukraine verübt.	22.10.2020“