BESCHLÜSSE

BESCHLUSS (GASP) 2020/1537 DES RATES

vom 22. Oktober 2020

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) 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 von solchen Aktivitäten abzuschrecken und darauf zu reagieren.

(3) Um fortgesetzte und zunehmende böswillige Handlungen im Cyberraum zu verhindern, von ihnen abzuschrecken und auf sie zu reagieren, sollten zwei natürliche Personen und eine Einrichtung in die im Anhang des Beschlusses (GASP) 2019/797 enthaltene Liste der natürlichen und juristischen Personen, Organisationen und Einrichtungen, gegen die restriktive Maßnahmen verhängt wurden, aufgenommen werden. Diese Personen und diese Einrichtung sind verantwortlich für Cyberangriffe mit erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen, — insbesondere für den Cyberangriff gegen den Deutschen Bundestag, der im April und im Mai 2015 stattfand — oder waren daran beteiligt.

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

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Der Anhang des Beschlusses (GASP) 2019/797 wird gemäß dem Anhang des vorliegenden Beschlusses geändert.

Artikel 2

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

Geschehen zu Brüssel am 22. Oktober 2020.

Im Namen des Rates
Der Präsident
M. ROTH

([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 129I vom 17.5.2019, S. 13).

ANHANG

Die folgenden Einträge werden in die Liste der natürlichen und juristischen Personen, Organisationen und Einrichtungen im Anhang des Beschlusses (GASP) 2019/797 aufgenommen:

A. Natürliche Personen

	Name	Angaben zur Identität	Gründe	Datum der Aufnahme in die Liste
„7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Geburtsdatum: 15. November 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 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 Bundeskanzlerin Angela Merkel waren betroffen.	22.10.2020
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Geburtsdatum: 21. Februar 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), auch bekannt als „Militäreinheit 26165“ (in Fachkreisen bekannt unter den Beinamen „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, der im April und Mai 2015 stattfand, 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 Bundeskanzlerin Angela Merkel waren betroffen.	22.10.2020“

B. Juristische Personen, Organisationen und Einrichtungen

	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)	Anschrift: 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), auch bekannt als „Militäreinheit 26165" bekannt (in Fachkreisen bekannt unter den Beinamen „APT28", „Fancy Bear", „Sofacy Group", „Pawn Storm" und „Strontium"), ist verantwortlich für Cyberangriffe 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, der im April und Mai 2015 stattfand, 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 Bundeskanzlerin Angela Merkel waren betroffen.	22.10.2020"