**Dieser Text dient lediglich zu Informationszwecken und hat keine Rechtswirkung. Die EU-Organe übernehmen keine Haftung für seinen Inhalt. Verbindliche Fassungen der betreffenden Rechtsakte einschließlich ihrer Präambeln sind nur die im Amtsblatt der Europäischen Union veröffentlichten und auf EUR-Lex verfügbaren Texte. Diese amtlichen Texte sind über die Links in diesem Dokument unmittelbar zugänglich**

►B

# 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)

Geändert durch:

| | | Amtsblatt | | |
|---|---|---|---|---|
| | | Nr. | Seite | Datum |
| ►M1 | Beschluss (GASP) 2020/651 des Rates vom 14. Mai 2020 | L 153 | 4 | 15.5.2020 |
| ►M2 | Beschluss (GASP) 2020/1127 des Rates vom 30. Juli 2020 | L 246 | 12 | 30.7.2020 |
| ►M3 | Beschluss (GASP) 2020/1537 des Rates vom 22. Oktober 2020 | L 351I | 5 | 22.10.2020 |
| ►M4 | Beschluss (GASP) 2020/1748 des Rates vom 20. November 2020 | L 393 | 19 | 23.11.2020 |
| ►M5 | Beschluss (GASP) 2021/796 des Rates vom 17. Mai 2021 | L 174I | 1 | 18.5.2021 |
| ►M6 | Beschluss (GASP) 2022/754 des Rates vom 16. Mai 2022 | L 138 | 16 | 17.5.2022 |
| ►M7 | Beschluss (GASP) 2023/964 des Rates vom 15. Mai 2023 | L 129 | 16 | 16.5.2023 |
| ►M8 | Beschluss (GASP) 2023/2686 des Rates vom 27. November 2023 | L 2686 | 1 | 28.11.2023 |
| ►M9 | Beschluss (GASP) 2024/1391 des Rates vom 17. Mai 2024 | L 1391 | 1 | 17.5.2024 |
| ►M10 | Beschluss (GASP) 2024/1779 des Rates vom 24. Juni 2024 | L 1779 | 1 | 24.6.2024 |
| ►M11 | Beschluss (GASP) 2025/171 des Rates vom 27. Januar 2025 | L 171 | 1 | 27.1.2025 |
| ►M12 | Beschluss (GASP) 2025/887 des Rates vom 12. Mai 2025 | L 887 | 1 | 13.5.2025 |
| ►M13 | Beschluss (GASP) 2026/588 des Rates vom 16. März 2026 | L 588 | 1 | 16.3.2026 |
| ►M14 | Beschluss (GASP) 2026/1079 des Rates vom 11. Mai 2026 | L 1079 | 1 | 12.5.2026 |

Berichtigt durch:

►C1 Berichtigung, ABl. L 230 vom 17.7.2020, S. 36 (2019/797)
►C2 Berichtigung, ABl. L 90401 vom 9.7.2024, S. 1 (2024/1779)

▼B

**BESCHLUSS (GASP) 2019/797 DES RATES**

**vom 17. Mai 2019**

**über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen**

*Artikel 1*

(1) Dieser Beschluss gilt für Cyberangriffe mit erheblichen Auswirkungen, einschließlich versuchter Cyberangriffe mit potenziell erheblichen Auswirkungen, die eine äußere Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.

(2) Zu Cyberangriffen, die eine äußere Bedrohung darstellen, zählen Cyberangriffe, die

a) ihren Ausgang außerhalb der Union haben oder von dort durchgeführt werden,

b) außerhalb der Union befindliche Infrastrukturen nutzen,

c) von natürlichen oder juristischen Personen, Organisationen oder Einrichtungen, die außerhalb der Union ansässig oder tätig sind, durchgeführt werden oder

d) mit Unterstützung, auf Anweisung oder unter der Kontrolle von natürlichen oder juristischen Personen, Organisationen oder Einrichtungen, die außerhalb der Union tätig sind, durchgeführt werden.

(3) Zu diesem Zweck sind Cyberangriffe Handlungen, die

a) den Zugang zu Informationssystemen,

b) den Eingriff in Informationssysteme,

c) den Eingriff in Daten oder

d) das Abfangen von Daten

umfassen, wenn diese Handlungen vom Eigentümer oder einem anderen Rechtsinhaber des Systems oder der Daten oder eines Teils des Systems oder der Daten nicht ordnungsgemäß gestattet wurden oder nach dem Recht der Union oder des betreffenden Mitgliedstaats nicht zulässig sind.

(4) Zu Cyberangriffen, die eine Bedrohung für die Mitgliedstaaten darstellen, zählen Cyberangriffe auf Informationssysteme, u. a. in den folgenden Bereichen:

a) kritische Infrastrukturen, einschließlich Seekabel und in den Weltraum gestarteter Gegenstände, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen oder der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind;

b) Dienstleistungen, die für die Aufrechterhaltung wesentlicher sozialer und/oder wirtschaftlicher Tätigkeiten erforderlich sind, insbesondere in den Sektoren: Energie (Elektrizität, Öl und Gas), Verkehr (Luft, Schiene, Wasser und Straße), Bankenwesen, Finanzmarktinfrastrukturen, Gesundheitswesen (Gesundheitsdienstleister, Krankenhäuser

▼B

und Privatkliniken), Trinkwasserlieferung und -versorgung oder digitale Infrastruktur und in anderen Sektoren, die für den betreffenden Mitgliedstaat von wesentlicher Bedeutung sind;

c) kritische staatliche Funktionen, insbesondere in den Bereichen Verteidigung, Staatsführung und Funktionieren der Institutionen, u. a. im Zusammenhang mit Wahlen oder dem Wahlvorgang, Funktionieren der wirtschaftlichen und der zivilen Infrastruktur, innere Sicherheit sowie Außenbeziehungen, einschließlich mittels diplomatischer Missionen;

d) Speicherung oder Verarbeitung von Verschlusssachen oder

e) Katastrophenstäbe der Regierungen.

(5) Zu Cyberangriffen, die eine Bedrohung für die Union darstellen, zählen Cyberangriffe, die gegen ihre Organe, Einrichtungen und sonstigen Stellen, ihre Delegationen in Drittstaaten oder bei internationalen Organisationen, ihre Operationen und Missionen im Bereich der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) und ihre Sonderbeauftragten geführt werden.

(6) Sofern dies für notwendig erachtet wird, um die in den einschlägigen Bestimmungen des Artikels 21 des Vertrags über die Europäische Union festgelegten Ziele der GASP zu erreichen, können restriktive Maßnahmen gemäß diesem Beschluss auch zur Reaktion auf gegen Drittstaaten oder internationale Organisationen gerichtete Cyberangriffe mit erheblichen Auswirkungen angewandt werden.

*Artikel 2*

Für die Zwecke dieses Beschlusses bezeichnet der Ausdruck

a) „Informationssysteme“ eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung von digitalen Daten durchführen, sowie die von ihr oder ihnen zum Zwecke des Betriebs, der Nutzung, des Schutzes und der Pflege gespeicherten, verarbeiteten, abgerufenen oder übertragenen digitalen Daten;

b) „Eingriff in Informationssysteme“ eine Behinderung oder Störung des Betriebs eines Informationssystems durch Eingeben von digitalen Daten, durch Übermitteln, Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von digitalen Daten oder durch Unzugänglichmachen von digitalen Daten;

c) „Eingriff in Daten“ das Löschen, Beschädigen, Beeinträchtigen, Verändern, Unterdrücken oder Unzugänglichmachen von digitalen Daten eines Informationssystems; hierunter fällt auch der Diebstahl von Daten, Geldern, wirtschaftlichen Ressourcen oder geistigem Eigentum;

d) „Abfangen von Daten“ das mit technischen Hilfsmitteln bewirkte Abfangen nichtöffentlicher digitaler Datenübermittlungen an ein Informationssystem, aus einem Informationssystem oder innerhalb eines Informationssystems, einschließlich elektromagnetischer Abstrahlungen aus einem Informationssystem, das Träger solcher digitaler Daten ist.

▼B

*Artikel 3*

Zu den Faktoren, anhand deren festgestellt wird, ob ein Cyberangriff erhebliche Auswirkungen im Sinne von Artikel 1 Absatz 1 hat, gehören die folgenden:

a) Umfang, Ausmaß, Wirkung oder Schwere der verursachten Störung, einschließlich für wirtschaftliche und gesellschaftliche Tätigkeiten, wesentliche Dienste, kritische staatliche Funktionen, die öffentliche Ordnung oder die öffentliche Sicherheit;

b) die Zahl der betroffenen natürlichen oder juristischen Personen, Organisationen oder Einrichtungen;

c) die Zahl der betroffenen Mitgliedstaaten;

d) die Höhe des wirtschaftlichen Schadens, der z. B. durch einen groß angelegten Diebstahl von Geldern, wirtschaftlichen Ressourcen oder geistigem Eigentum verursacht wurde;

e) der vom Täter für sich selbst oder für andere erlangte wirtschaftliche Nutzen;

f) die Menge oder Art der gestohlenen Daten oder das Ausmaß der Datenschutzverstöße oder

g) die Art der wirtschaftlich sensiblen Daten, auf die zugegriffen wurde.

*Artikel 4*

(1) Die Mitgliedstaaten ergreifen die erforderlichen Maßnahmen, um folgende Personen an der Einreise in oder der Durchreise durch ihr Hoheitsgebiet zu hindern:

a) natürliche Personen, die für Cyberangriffe oder versuchte Cyberangriffe verantwortlich sind,

b) natürliche Personen, die finanzielle, technische oder materielle Unterstützung für Cyberangriffe oder versuchte Cyberangriffe leisten oder auf andere Weise, einschließlich durch Planung, Vorbereitung, Mitwirkung, Steuerung, Unterstützung oder Ermutigung, daran beteiligt sind oder sie durch Handlung oder Unterlassung erleichtern,

c) natürliche Personen, die mit den unter den Buchstaben a und b genannten natürlichen Personen in Verbindung stehen,

wie im Anhang aufgeführt.

(2) Absatz 1 verpflichtet die Mitgliedstaaten nicht dazu, ihren eigenen Staatsangehörigen die Einreise in ihr Hoheitsgebiet zu verweigern.

(3) Absatz 1 lässt die Fälle unberührt, in denen für einen Mitgliedstaat eine völkerrechtliche Verpflichtung besteht, und zwar

a) als Gastland einer internationalen zwischenstaatlichen Organisation,

b) als Gastland einer internationalen Konferenz, die von den Vereinten Nationen einberufen wurde oder unter ihrer Schirmherrschaft steht,

c) im Rahmen eines multilateralen Übereinkommens, das Vorrechte und Immunitäten verleiht, oder

d) im Rahmen des 1929 zwischen dem Heiligen Stuhl (Staat Vatikanstadt) und Italien geschlossenen Lateranvertrags.

▼B

(4) Absatz 3 gilt auch in den Fällen, in denen ein Mitgliedstaat Gastland der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) ist.

(5) Der Rat ist in allen Fällen, in denen ein Mitgliedstaat eine Ausnahme aufgrund von Absatz 3 oder 4 gewährt, ordnungsgemäß zu unterrichten.

(6) Die Mitgliedstaaten können Ausnahmen von den Maßnahmen nach Absatz 1 in den Fällen zulassen, in denen die Reise aufgrund einer humanitären Notlage oder aufgrund der Teilnahme an Tagungen auf zwischenstaatlicher Ebene oder an Tagungen, die von der Union unterstützt oder ausgerichtet werden oder aber von einem Mitgliedstaat, der zu dem Zeitpunkt den OSZE-Vorsitz inne hat, ausgerichtet werden, gerechtfertigt ist, wenn dort ein politischer Dialog geführt wird, der die politischen Zielen der restriktiven Maßnahmen, einschließlich der Sicherheit und Stabilität im Cyberraum, unmittelbar fördert.

(7) Mitgliedstaaten können auch dann Ausnahmen von den Maßnahmen nach Absatz 1 zulassen, wenn die Einreise oder Durchreise für die Teilnahme an einem Gerichtsverfahren notwendig ist.

(8) Ein Mitgliedstaat, der Ausnahmen nach Absatz 6 oder 7 zulassen möchte, unterrichtet den Rat schriftlich hiervon. Die Ausnahme gilt als gewährt, wenn nicht von einem oder mehreren Mitgliedern des Rates innerhalb von zwei Arbeitstagen nach Eingang der Mitteilung über die vorgeschlagene Ausnahme schriftlich Einwand erhoben wird. Wenn von einem oder mehreren Mitgliedern des Rates Einwand erhoben wird, so kann der Rat mit qualifizierter Mehrheit beschließen, die vorgeschlagene Ausnahme zu gewähren.

(9) In den Fällen, in denen ein Mitgliedstaat den im Anhang aufgeführten Personen die Einreise in sein Hoheitsgebiet oder die Durchreise durch sein Hoheitsgebiet nach Absatz 3, 4, 6, 7 oder 8 genehmigt, gilt die Genehmigung nur für den Zweck, für den sie erteilt wurde, und für die davon unmittelbar betroffenen Personen.

*Artikel 5*

(1) Sämtliche Gelder und wirtschaftlichen Ressourcen im Besitz, im Eigentum, in der Verfügungsgewalt oder unter der Kontrolle von

a) natürlichen oder juristischen Personen, Organisationen oder Einrichtungen, die für Cyberangriffe oder versuchte Cyberangriffe verantwortlich sind,

b) natürlichen oder juristischen Personen, Organisationen oder Einrichtungen, die finanzielle, technische oder materielle Unterstützung für Cyberangriffe oder versuchte Cyberangriffe leisten oder auf andere Weise, einschließlich durch Planung, Vorbereitung, Mitwirkung, Steuerung, Unterstützung oder Ermutigung, daran beteiligt sind oder sie durch Handlung oder Unterlassung erleichtern,

c) natürlichen oder juristischen Personen, Organisationen oder Einrichtungen, die mit den unter den Buchstaben a und b genannten natürlichen oder juristischen Personen, Organisationen oder Einrichtungen in Verbindung stehen,

wie im Anhang aufgeführt, werden eingefroren.

▼B

(2) Den im Anhang aufgeführten natürlichen oder juristischen Personen, Organisationen oder Einrichtungen dürfen weder unmittelbar noch mittelbar Gelder oder wirtschaftliche Ressourcen zur Verfügung gestellt werden oder zugutekommen.

(3) Abweichend von den Absätzen 1 und 2 können die zuständigen Behörde der Mitgliedstaaten die Freigabe bestimmter eingefrorener Gelder oder wirtschaftlicher Ressourcen oder die Zurverfügungstellung bestimmter Gelder oder wirtschaftlicher Ressourcen unter ihnen angemessen erscheinenden Bedingungen genehmigen, nachdem festgestellt wurde, dass die betreffenden Gelder oder wirtschaftlichen Ressourcen

a) ►C1 zur Befriedigung der Grundbedürfnisse der im Anhang genannten natürlichen oder juristischen Personen, Organisationen oder Einrichtungen, und ◄ der unterhaltsberechtigten Familienangehörigen jener natürlichen Personen, unter anderem für die Bezahlung von Nahrungsmitteln, Mieten oder Hypotheken, Medikamenten und medizinischer Behandlung, Steuern, Versicherungsprämien und Gebühren öffentlicher Versorgungseinrichtungen, erforderlich sind;

b) ausschließlich der Bezahlung angemessener Honorare oder der Rückerstattung von Ausgaben im Zusammenhang mit der Bereitstellung rechtlicher Dienste dienen;

c) ausschließlich der Bezahlung von Gebühren oder Kosten für die routinemäßige Verwahrung oder Verwaltung eingefrorener Gelder oder wirtschaftlicher Ressourcen dienen;

d) für die Deckung außerordentlicher Ausgaben erforderlich sind, vorausgesetzt, dass die relevante zuständige Behörde den zuständigen Behörden der anderen Mitgliedstaaten und der Kommission mindestens zwei Wochen vor Erteilung der Genehmigung mitgeteilt hat, aus welchen Gründen sie der Auffassung ist, dass eine spezifische Genehmigung erteilt werden sollte; oder

e) auf Konten oder von Konten einer diplomatischen Vertretung oder einer Konsularstelle oder einer internationalen Organisation überwiesen werden sollen, die Immunität nach dem Völkerrecht genießt, sofern diese Zahlungen für amtliche Zwecke dieser diplomatischen Vertretung oder Konsularstelle oder internationalen Organisation bestimmt sind.

Der betreffende Mitgliedstaat unterrichtet die anderen Mitgliedstaaten und die Kommission über jede nach diesem Absatz erteilte Genehmigung.

(4) Abweichend von Absatz 1 können die zuständigen Behörden der Mitgliedstaaten die Freigabe bestimmter eingefrorener Gelder oder wirtschaftlicher Ressourcen genehmigen, wenn die nachstehenden Voraussetzungen erfüllt sind:

a) Die Gelder oder wirtschaftlichen Ressourcen sind Gegenstand einer schiedsgerichtlichen Entscheidung, die vor dem Datum ergangen ist, an dem die in Absatz 1 genannte natürliche oder juristische Person, Organisation oder Einrichtung in den Anhang aufgenommen wurde, oder Gegenstand einer vor oder nach diesem Datum in der Union ergangenen gerichtlichen oder behördlichen Entscheidung oder einer in dem betreffenden Mitgliedstaat vollstreckbaren gerichtlichen Entscheidung;

▼B

b) die Gelder oder wirtschaftlichen Ressourcen werden im Rahmen der anwendbaren Gesetze und sonstigen Rechtsvorschriften über die Rechte des Gläubigers ausschließlich zur Erfüllung der Forderungen verwendet, die durch eine solche Entscheidung gesichert sind oder deren Bestehen in einer solchen Entscheidung bestätigt worden ist;

c) die Entscheidung begünstigt nicht eine im Anhang aufgeführte natürliche oder juristische Person, Organisation oder Einrichtung; und

d) die Anerkennung der Entscheidung steht nicht im Widerspruch zur öffentlichen Ordnung des betreffenden Mitgliedstaats.

Der betreffende Mitgliedstaat unterrichtet die anderen Mitgliedstaaten und die Kommission über jede nach diesem Absatz erteilte Genehmigung.

(5) Absatz 1 hindert eine im Anhang aufgeführte natürliche oder juristische Person, Organisation oder Einrichtung nicht daran, Zahlungen aufgrund eines Vertrags zu leisten, der vor dem Zeitpunkt eingegangen wurde, zu dem diese natürliche oder juristische Person, Organisation oder Einrichtung in den Anhang aufgenommen wurde, sofern der jeweilige Mitgliedstaat festgestellt hat, dass die Zahlung weder unmittelbar noch mittelbar von einer natürlichen oder juristischen Person, Organisation oder Einrichtung im Sinne von Absatz 1 entgegengenommen wird.

(6) Absatz 2 gilt nicht für die auf eingefrorenen Konten eingehenden

a) Zinsen und sonstigen Erträge dieser Konten,

b) Zahlungen aufgrund von Verträgen, Vereinbarungen oder Verpflichtungen, die vor dem Zeitpunkt eingegangen wurden, ab dem diese Konten den Maßnahmen nach den Absätzen 1 und 2 unterliegen, oder

c) Zahlungen aufgrund von in der Union ergangenen oder in dem betreffenden Mitgliedstaat vollstreckbaren gerichtlichen, behördlichen oder schiedsgerichtlichen Entscheidungen,

sofern solche Zinsen, sonstigen Erträge und Zahlungen weiterhin den Maßnahmen nach Absatz 1 unterliegen.

▼M8

(7) Die Absätze 1 und 2 finden keine Anwendung auf die Bereitstellung von Geldern oder wirtschaftlichen Ressourcen, die notwendig sind, um die rasche Bereitstellung humanitärer Hilfe zu gewährleisten oder andere Tätigkeiten zur Deckung grundlegender menschlicher Bedürfnisse zu unterstützen, wenn die Hilfe bzw. die anderen Tätigkeiten durchgeführt werden von

a) den Vereinten Nationen (VN), einschließlich ihrer Programme, Gelder und sonstigen Einrichtungen und Stellen, sowie ihren Sonderorganisationen und verwandten Organisationen,

b) internationalen Organisationen,

▼M8

c) humanitäre Hilfe leistenden Organisationen mit Beobachterstatus in der Generalversammlung der VN und Mitgliedern dieser Organisationen,

d) bilateral oder multilateral finanzierten nichtstaatlichen Organisationen, die sich an den Plänen der VN für humanitäre Maßnahmen, den Plänen der VN für Flüchtlingshilfemaßnahmen oder anderen Appellen der VN oder an vom Amt der VN für die Koordinierung humanitärer Angelegenheiten koordinierten humanitären „Clustern“ beteiligen,

e) Organisationen und Agenturen, denen die Union das Zertifikat für humanitäre Partnerschaft erteilt hat oder die von einem Mitgliedstaat als Partner für humanitäre Hilfe nach nationalen Verfahren zertifiziert oder anerkannt sind,

f) spezialisierten Agenturen der Mitgliedstaaten oder

g) den Beschäftigten, Zuschussempfängern, Tochtergesellschaften oder Durchführungspartnern der unter den Buchstaben a bis f genannten Einrichtungen, während und soweit sie in dieser Eigenschaft tätig sind.

(8) Unbeschadet des Absatzes 7 können die zuständigen Behörden der Mitgliedstaaten abweichend von den Absätzen 1 und 2 unter ihnen geeignet erscheinenden Bedingungen die Freigabe bestimmter eingefrorener Gelder oder wirtschaftlicher Ressourcen oder die Bereitstellung bestimmter Gelder oder wirtschaftlicher Ressourcen genehmigen, nachdem sie festgestellt haben, dass die Zurverfügungstellung dieser Gelder oder wirtschaftlichen Ressourcen notwendig ist, um die rasche Bereitstellung humanitärer Hilfe zu gewährleisten oder andere Tätigkeiten zur Deckung grundlegender menschlicher Bedürfnisse zu unterstützen.

(9) Ergeht innerhalb von fünf Arbeitstagen nach Eingang des Genehmigungsantrags nach Absatz 8 keine ablehnende Entscheidung, kein Auskunftsersuchen oder keine Mitteilung über eine Fristverlängerung der einschlägigen zuständigen Behörde, so gilt die Genehmigung als erteilt.

(10) Der betreffende Mitgliedstaat unterrichtet die anderen Mitgliedstaaten und die Kommission über nach den Absätzen 8 und 9 erteilte Genehmigungen innerhalb von vier Wochen nach einer solchen Erteilung.

▼B

*Artikel 6*

(1) Auf Vorschlag eines Mitgliedstaats oder des Hohen Vertreters der Union für Außen- und Sicherheitspolitik erstellt und ändert der Rat einstimmig die im Anhang enthaltene Liste.

(2) Der Rat setzt die betreffende natürliche oder juristische Person, Organisation oder Einrichtung entweder auf direktem Weg, falls ihre Anschrift bekannt ist, oder durch die Veröffentlichung einer Bekanntmachung von dem Beschluss nach Absatz 1 und den Gründen für die Aufnahme in die Liste in Kenntnis und gibt dabei dieser natürlichen oder juristischen Person, Organisation oder Einrichtung Gelegenheit zur Stellungnahme.

▼B

(3) Wird eine Stellungnahme unterbreitet oder werden stichhaltige neue Beweise vorgelegt, so überprüft der Rat den Beschluss nach Absatz 1 und unterrichtet die betreffende natürliche oder juristische Person, Organisation oder Einrichtung entsprechend.

*Artikel 7*

(1) Im Anhang werden die Gründe für die Aufnahme der natürlichen und juristischen Personen, Organisationen und Einrichtungen nach den Artikeln 4 und 5 in die Liste angegeben.

(2) Der Anhang enthält die zur Identifizierung der betreffenden natürlichen oder juristischen Personen, Organisationen oder Einrichtungen erforderlichen Angaben, soweit diese verfügbar sind. Bei natürlichen Personen können diese Angaben Namen und Aliasnamen, Geburtsdatum und -ort, Staatsangehörigkeit, Reisepass- und Personalausweisnummern, Geschlecht, Anschrift, soweit bekannt, und Funktion oder Beruf umfassen. Bei juristischen Personen, Organisationen oder Einrichtungen können diese Angaben Namen, Ort und Datum der Registrierung, Registriernummer und Geschäftssitz umfassen.

*Artikel 8*

Ansprüche im Zusammenhang mit Verträgen oder Transaktionen, deren Erfüllung bzw. Durchführung von den mit diesem Beschluss verhängten Maßnahmen unmittelbar oder mittelbar, ganz oder teilweise betroffen ist, einschließlich Schadensersatzansprüchen und ähnlichen Ansprüchen, wie etwa Entschädigungsansprüche oder Garantieansprüche, vor allem Ansprüche auf Verlängerung oder Zahlung einer insbesondere finanziellen Garantie oder Gegengarantie in jeglicher Form, werden nicht erfüllt, sofern sie geltend gemacht werden von

a) den benannten, im Anhang aufgeführten natürlichen oder juristischen Personen, Organisationen oder Einrichtungen,

b) natürlichen oder juristischen Personen, Organisationen oder Einrichtungen, die über eine der unter Buchstabe a genannten natürlichen oder juristischen Personen, Organisationen oder Einrichtungen oder in deren Namen handeln.

*Artikel 9*

Damit die in diesem Beschluss vorgesehenen Maßnahmen größtmögliche Wirkung entfalten können, empfiehlt die Union Drittstaaten, restriktive Maßnahmen zu ergreifen, die mit den in diesem Beschluss vorgesehenen restriktiven Maßnahmen vergleichbar sind.

▼M14

*Artikel 10*

Dieser Beschluss gilt bis zum 18. Mai 2028 und wird fortlaufend überprüft. Die in den Artikeln 4 und 5 genannten Maßnahmen gelten für die im Anhang aufgeführten natürlichen und juristischen Personen, Organisationen und Einrichtungen bis zum 18. Mai 2027.

▼B

*Artikel 11*

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

▼B

*ANHANG*

**Liste der natürlichen und juristischen Personen, Organisationen und Einrichtungen gemäß den Artikeln 4 und 5**

▼M2

A. Natürliche Personen

▼M14

| | Name | Angaben zur Identität | Gründe | Datum der Aufnahme in die Liste |
|---|---|---|---|---|
| 1. | GAO Qiang | Geburtsdatum: 4. Oktober 1983<br>Geburtsort: Provinz Shandong, China<br>Anschrift: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China<br>Staatsangehörigkeit: chinesisch<br>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.<br>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.<br>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 |
| 2. | ZHANG Shilong | Geburtsdatum: 10. September 1981<br>Geburtsort: China<br>Anschrift: Anschrift: Hedong, Yuyang Road No 121, Tianjin, China<br>Staatsangehörigkeit: chinesisch<br>Geschlecht: männlich | Zhang Shilong 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. | 30.7.2020 |

02019D0797 — DE — 13.05.2026 — 014.001 — 10

▼M14

| | Name | Angaben zur Identität | Gründe | Datum der Aufnahme in die Liste |
|---|---|---|---|---|
| | | | 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.<br>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.<br>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.<br>Er steht ferner in Verbindung mit Gao Qiang, der mit APT10 in Verbindung gebracht wird und der auch bei Huaying Haitai beschäftigt ist. | |

▼M12

| | | | | |
|---|---|---|---|---|
| 3. | Alexey Valeryevich MININ | Алексей Валерьевич МИНИН<br>Geburtsdatum: 27.5.1972<br>Geburtsort: Oblast Perm, Russische SFSR (jetzt Russische Föderation)<br>Reisepass-Nr.: 120017582<br>ausgestellt vom Außenministerium der Russischen Föderation<br>gültig vom 17.4.2017 bis zum 17.4.2022<br>Ort: Moskau, Russische Föderation<br>Staatsangehörigkeit: russisch<br>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.<br>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.<br>Eine Grand Jury des Western District of Pennsylvania (Vereinigte Staaten von Amerika) hat Alexey Minin als Beamter der GRU wegen Computerhackings, Telekommunikationsbetrugs, schweren Identitätsdiebstahls und Geldwäsche angeklagt. | 30.7.2020 |

▼M12

| | Name | Angaben zur Identität | Gründe | Datum der Aufnahme in die Liste |
|---|---|---|---|---|
| | | | Die GRU führt weiterhin aktiv Cyberangriffe gegen die Union oder ihre Mitgliedstaaten durch. Als Mitglied der GRU ist Alexey Minin daher an Cyberangriffen mit erheblichen Auswirkungen beteiligt, einschließlich versuchter Cyberangriffe mit potenziell erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen. | |
| 4. | Aleksei Sergeyvich MORENETS | Алексей Сергеевич МОРЕНЕЦ<br>Geburtsdatum: 31.7.1977<br>Geburtsort: Oblast Murmansk, Russische SFSR (jetzt Russische Föderation)<br>Reisepass-Nr.: 100135556<br>ausgestellt vom Außenministerium der Russischen Föderation<br>gültig vom 17.4.2017 bis zum 17.4.2022<br>Ort: Moskau, Russische Föderation<br>Staatsangehörigkeit: russisch<br>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.<br>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.<br>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.<br>Die GRU führt weiterhin aktiv Cyberangriffe gegen die Union oder ihre Mitgliedstaaten durch. Als Mitglied der GRU ist Aleksei Morenets daher an Cyberangriffen mit erheblichen Auswirkungen beteiligt, einschließlich versuchter Cyberangriffe mit potenziell erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen. | 30.7.2020 |

02019D0797 — DE — 13.05.2026 — 014.001 — 12

▼M12

| | Name | Angaben zur Identität | Gründe | Datum der Aufnahme in die Liste |
|---|---|---|---|---|
| 5. | Evgenii Mikhaylovich SEREBRIAKOV | Евгений Михайлович СЕРЕБРЯКОВ<br>Geburtsdatum: 26.7.1981<br>Geburtsort: Kursk, Russische SFSR (jetzt Russische Föderation)<br>Reisepass-Nr.: 100135555<br>ausgestellt vom Außenministerium der Russischen Föderation<br>gültig vom 17.4.2017 bis zum 17.4.2022<br>Ort: Moskau, Russische Föderation<br>Staatsangehörigkeit: russisch<br>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.<br>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.<br>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.<br>Die GRU führt weiterhin aktiv Cyberangriffe gegen die Union oder ihre Mitgliedstaaten durch. Als Mitglied der GRU ist Evgenii Serebriakov daher an Cyberangriffen mit erheblichen Auswirkungen beteiligt, einschließlich versuchter Cyberangriffe mit potenziell erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen. | 30.7.2020 |

▼M12

| | Name | Angaben zur Identität | Gründe | Datum der Aufnahme in die Liste |
|---|---|---|---|---|
| 6. | Oleg Mikhaylovich SOTNIKOV | Олег Михайлович СОТНИКОВ<br>Geburtsdatum: 24.8.1972<br>Geburtsort: Uljanowsk, Russische SFSR (jetzt Russische Föderation)<br>Reisepass-Nr.: 120018866<br>ausgestellt vom Außenministerium der Russischen Föderation<br>gültig vom 17.4.2017 bis zum 17.4.2022<br>Ort: Moskau, Russische Föderation<br>Staatsangehörigkeit: russisch<br>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.<br>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.<br>Eine Grand Jury des Western District of Pennsylvania (Vereinigte Staaten von Amerika) hat Oleg Sotnikov als Beamter der GRU wegen Computerhackings, Telekommunikationsbetrugs, schweren Identitätsdiebstahls und Geldwäsche angeklagt.<br>Die GRU führt weiterhin aktiv Cyberangriffe gegen die Union oder ihre Mitgliedstaaten durch. Als Mitglied der GRU ist Oleg Sotnikov daher an Cyberangriffen mit erheblichen Auswirkungen beteiligt, einschließlich versuchter Cyberangriffe mit potenziell erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen. | 30.7.2020 |

▼M12

| | Name | Angaben zur Identität | Gründe | Datum der Aufnahme in die Liste |
|---|---|---|---|---|
| 7. | Dmitry Sergeyevich BADIN | Дмитрий Сергеевич БАДИН<br>Geburtsdatum: 15.11.1990<br>Geburtsort: Kursk, Russische SFSR (jetzt Russische Föderation)<br>Staatsangehörigkeit: russisch<br>Geschlecht: männlich | Dmitry Badin war an einem Cyberangriff mit erheblichen Auswirkungen gegen den Deutschen Bundestag sowie an Cyberangriffen mit erheblichen Auswirkungen auf Drittstaaten beteiligt.<br>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.<br>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.<br>Die GRU führt weiterhin aktiv Cyberangriffe gegen die Union oder ihre Mitgliedstaaten durch. Als Mitglied der GRU ist Dmitry Badin daher an Cyberangriffen mit erheblichen Auswirkungen beteiligt, einschließlich versuchter Cyberangriffe mit potenziell erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen. | 22.10.2020 |
| 8. | Igor Olegovich KOSTYUKOV | Игорь Олегович КОСТЮКОВ<br>Geburtsdatum: 21.2.1961<br>Staatsangehörigkeit: russisch<br>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“).<br>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. | 22.10.2020 |

▼M12

| | Name | Angaben zur Identität | Gründe | Datum der Aufnahme in die Liste |
|---|---|---|---|---|
| | | | 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.<br>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.<br>Die GRU führt weiterhin aktiv Cyberangriffe gegen die Union oder ihre Mitgliedstaaten durch. Als Mitglied der GRU ist Igor Kostyukov daher an Cyberangriffen mit erheblichen Auswirkungen beteiligt, einschließlich versuchter Cyberangriffe mit potenziell erheblichen Auswirkungen, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen. | |

▼M10

| | | | | |
|---|---|---|---|---|
| 9. | Ruslan Aleksandrovich PERETYATKO | Руслан Александрович ПЕРЕТЯТЬКО<br>Geburtsdatum: 3.8.1985<br>Staatsangehörigkeit: russisch<br>Geschlecht: männlich | Ruslan PERETYATKO war an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.<br>►C2 Ruslan PERETYATKO gehört der „Callisto“-Gruppe an, einer Gruppe von Beamten des russischen Geheimdienstes, die Cyberoperationen gegen Mitgliedstaaten der EU und Drittstaaten durchführt. ◄<br>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.<br>Deshalb ist Ruslan PERETYATKO an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen. | 24.6.2024 |

▼M10

| | Name | Angaben zur Identität | Gründe | Datum der Aufnahme in die Liste |
|---|---|---|---|---|
| 10. | Andrey Stanislavovich KORINETS | Андрей Станиславович КОРИНЕЦ<br>Geburtsdatum: 18.5.1987<br>Geburtsort: Stadt Syktyvkar, Russland<br>Staatsangehörigkeit: russisch<br>Geschlecht: männlich | Andrey Stanislavovich KORINETS war an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.<br>Andrey Stanislavovich KORINETS ist Offizier des „Center 18“ des Inlandsgeheimdienstes der Russischen Föderation. ►C2 Andrey Stanislavovich KORINETS gehört der „Callisto-Gruppe“ an, einer Gruppe von Beamten des russischen Geheimdienstes, die Cyberoperationen gegen Mitgliedstaaten der EU und Drittstaaten durchführt. ◄<br>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.<br>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 |
| 11. | Oleksandr SKLIANKO | Александр СКЛЯНКО (russische Schreibweise)<br>Олександр СКЛЯНКО (ukrainische Schreibweise)<br>Geburtsdatum: 5.8.1973<br>Reisepass: EC 867868, ausgestellt am 27.11.1998 (Ukraine)<br>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.<br>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. | 24.6.2024 |

▼M10

| | Name | Angaben zur Identität | Gründe | Datum der Aufnahme in die Liste |
|---|---|---|---|---|
| | | | 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. | |
| 12. | Mykola CHERNYKH | Николай ЧЕРНЫХ (russische Schreibweise)<br>Микола ЧЕРНИХ (ukrainische Schreibweise)<br>Geburtsdatum: 12.10.1978<br>Reisepass: EC 922162, ausgestellt am 20.1.1999 (Ukraine)<br>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.<br>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.<br>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.<br>Deshalb ist Mykola CHERNYKH an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen. | 24.6.2024 |

▼M14

| | | | | |
|---|---|---|---|---|
| 13. | Mikhail Mikhailovich TSAREV | Михаил Михайлович ЦАРЕВ<br>Geburtsdatum: 20.4.1989<br>Geburtsort: Serpukhov, Russische Föderation<br>Staatsangehörigkeit: russisch<br>Anschrift: Serpukhov<br>Geschlecht: männlich | Mikhail Mikhailovich Tsarev war an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Mitgliedstaaten der EU darstellen.<br>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. | 24.6.2024 |

▼M14

| | Name | Angaben zur Identität | Gründe | Datum der Aufnahme in die Liste |
|---|---|---|---|---|
| | | | 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.<br>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.<br>Deshalb ist Mikhail Mikhailovich Tsarev an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen. | |
| 14. | Maksim Sergeevich GALOCHKIN | Максим Сергеевич ГАЛОЧКИН<br>Geburtsdatum: 19.5.1982<br>Geburtsort: Abakan, Russische Föderation<br>Staatsangehörigkeit: russisch<br>Geschlecht: männlich | Maksim Galochkin hat an Cyberangriffen mit erheblichen Auswirkungen mitgewirkt, die eine externe Bedrohung für die Mitgliedstaaten der EU darstellen.<br>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.<br>„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.<br>Deshalb ist Maksim Galochkin an Cyberangriffen mit erheblichen Auswirkungen beteiligt, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen. | 24.6.2024 |

▼M2

| | Name | Angaben zur Identität | Gründe | Datum der Aufnahme in die Liste |
|---|---|---|---|---|
| ▼M11 | | | | |
| 15. | Nikolay Alexandrovich KORCHAGIN | Николай Александрович Корчагин<br>Geburtsdatum: 16.9.1997<br>Staatsangehörigkeit: russisch<br>Geschlecht: männlich<br>Verbundene Organisation: Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation | Nikolay Korchagin ist an Cyberangriffen mit erheblichen Auswirkungen beteiligt und dafür verantwortlich, indem er nachrichtendienstliche Aktivitäten gegen Estland durchführt und sich illegal Zugang zu einem Computersystem verschafft hat.<br>Nikolay Korchagin ist Offizier der Militäreinheit 29155 der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GRU). In dieser Funktion ist er an Cyberangriffen auf Computersysteme beteiligt und dafür verantwortlich mit dem Ziel, Daten von den Datensystemen mehrerer Institutionen abzugreifen, die unabhängig voneinander oder in Kombination miteinander einen Überblick über die Cybersicherheitspolitik Estlands, die Cyberfähigkeiten des Staates, sensible personenbezogene Daten und andere sensible Daten gewähren, mit dem Ziel, die Daten zu verwenden, um die Sicherheit Estlands zu bedrohen. Die Angriffe betreffen daher die Speicherung von Verschlusssachen. Die Angriffe betrafen Verbündete und Partner Estlands.<br>Somit ist Nikolay Korchagin an Cyberangriffen mit erheblichen Auswirkungen, die eine äußere Bedrohung für einen Mitgliedstaat darstellen, beteiligt und dafür verantwortlich. | 27.1.2025 |
| 16. | Vitaly SHEVCHENKO | Виталий Шевченко<br>Geburtsdatum: 1.9.1997<br>Staatsangehörigkeit: russisch<br>Geschlecht: männlich<br>Verbundene Organisation: Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation | Vitaly Shevchenko ist an Cyberangriffen mit erheblichen Auswirkungen beteiligt und dafür verantwortlich, indem er nachrichtendienstliche Aktivitäten gegen Estland durchführt und sich illegal Zugang zu einem Computersystem verschafft hat.<br>Vitaly Shevchenko ist Offizier der Militäreinheit 29155 der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GRU). In dieser Funktion ist er an Cyberangriffen auf Computersysteme beteiligt und dafür verantwortlich mit dem Ziel, Daten von den Datensystemen mehrerer Institutionen abzugreifen, die unabhängig voneinander oder in Kombination miteinander einen Überblick über die Cybersicherheitspolitik Estlands, die Cyberfähigkeiten des Staates, sensible personenbezogene Daten und andere sensible Daten gewähren, mit dem Ziel, die Daten zu verwenden, um die Sicherheit Estlands zu bedrohen. Die Angriffe betreffen daher die Speicherung von Verschlusssachen. Die Angriffe betrafen Verbündete und Partner Estlands.<br>Somit ist Vitaly Shevchenko an Cyberangriffen mit erheblichen Auswirkungen, die eine äußere Bedrohung für einen Mitgliedstaat darstellen, beteiligt und dafür verantwortlich. | 27.1.2025 |

02019D0797 — DE — 13.05.2026 — 014.001 — 20

▼M11

| | Name | Angaben zur Identität | Gründe | Datum der Aufnahme in die Liste |
|---|---|---|---|---|
| 17. | Yuriy Fedorovich DENISOV | Юрий Федорович Денисов<br>Geburtsdatum: 17.6.1980<br>Staatsangehörigkeit: russisch<br>Geschlecht: männlich<br>Verbundene Organisation: Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation | Yuriy Denisov ist an Cyberangriffen mit erheblichen Auswirkungen beteiligt und dafür verantwortlich, indem er nachrichtendienstliche Aktivitäten gegen Estland durchführt und sich illegal Zugang zu einem Computersystem verschafft hat.<br>Yuriy Denisov ist Offizier der Militäreinheit 29155 der Hauptdirektion des Generalstabs der Streitkräfte der Russischen Föderation (GRU). In dieser Funktion ist er an Cyberangriffen auf Computersysteme beteiligt und dafür verantwortlich mit dem Ziel, Daten von den Datensystemen mehrerer Institutionen abzugreifen, die unabhängig voneinander oder in Kombination miteinander einen Überblick über die Cybersicherheitspolitik Estlands, die Cyberfähigkeiten des Staates, sensible personenbezogene Daten und andere sensible Daten gewähren, mit dem Ziel, die Daten zu verwenden, um die Sicherheit Estlands zu bedrohen. Die Angriffe betreffen daher die Speicherung von Verschlusssachen. Die Angriffe betrafen Verbündete und Partner Estlands.<br>Somit ist Yuriy Denisov an Cyberangriffen mit erheblichen Auswirkungen, die eine äußere Bedrohung für einen Mitgliedstaat darstellen, beteiligt und dafür verantwortlich. | 27.1.2025 |

▼M13

| | | | | |
|---|---|---|---|---|
| 18. | Chen Cheng | 陈诚<br>(chinesische Schreibweise)<br>Aliasnamen:<br>Jesse Chen<br>lengmo<br>l3n6m0<br>Geburtsdatum: 20.10.1984<br>Geburtsort: Yancheng, Jiangsu, China<br>Staatsangehörigkeit: chinesisch<br>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.<br>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.<br>Anxun Information Technology Co. Ltd. profitiert wirtschaftlich erheblich von den erbrachten Dienstleistungen. | 16.3.2026 |

▼M13

| | Name | Angaben zur Identität | Gründe | Datum der Aufnahme in die Liste |
|---|---|---|---|---|
| | | | 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.<br>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. | |
| 19. | Wu Haibo | 吴海波<br>(chinesische Schreibweise)<br>Aliasnamen:<br>shutdown<br>shutd0wn<br>Geburtsort: China<br>Staatsangehörigkeit: chinesisch<br>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.<br>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.<br>Anxun Information Technology Co. Ltd. profitiert wirtschaftlich erheblich von den erbrachten Dienstleistungen.<br>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.<br>Wu Haibo war an der Steuerung versuchter Cyberangriffe mit erheblichen Auswirkungen auf Mitgliedstaaten und an der Ermutigung dazu beteiligt.<br>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 |

▼M2

B. Juristische Personen, Organisationen und Einrichtungen

| | Name | Angaben zur Identität | Gründe | Datum der Aufnahme in die Liste |
|---|---|---|---|---|
| ▼M14 | | | | |
| 1. | Tianjin Huaying Haitai Science and Technology Development Co Ltd (Huaying Haitai) | Aliasname: Haitai Technology Development Co. Ltd<br>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.<br>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.<br>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.<br>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 |
| ▼M2 | | | | |
| 2. | Chosun Expo | Aliasname: Chosen Expo; Korea Export Joint Venture<br>Ort: DVRK | Die Chosun Expo hat 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, finanziell, technisch oder materiell unterstützt; dazu zählen die als „WannaCry“ bekannten Cyberangriffe und Cyberangriffe auf die polnische Finanzaufsichtsbehörde und auf Sony Pictures Entertainment sowie Cyberdiebstahl bei der Bangladesh Bank und versuchter Cyberdiebstahl bei der Vietnam Tien Phong Bank. | 30.7.2020 |

▼M2

| | Name | Angaben zur Identität | Gründe | Datum der Aufnahme in die Liste |
|---|---|---|---|---|
| | | | „WannaCry“ hat Störungen in Informationssystemen auf der ganzen Welt verursacht, indem Ransomware in Informationssysteme eingeschleust und der Zugriff auf Daten blockiert wurde. Betroffen waren Informationssysteme von Unternehmen in der Union, darunter Informationssysteme in Bezug auf Dienste, die für die Aufrechterhaltung wesentlicher Dienstleistungen und wirtschaftlicher Tätigkeiten in den Mitgliedstaaten erforderlich sind.<br>„WannaCry“ wurde von dem als „APT38“ („Advanced Persistent Threat 38“) bekannten Täter oder der „Lazarus Group“ verübt.<br>Die Chosun Expo kann mit APT38/der Lazarus Group in Verbindung gebracht werden, auch durch die bei den Cyberangriffen benutzten Konten. | |

▼M9

| | | | | |
|---|---|---|---|---|
| 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.<br>„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.<br>„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 | 30.7.2020 |

▼M9

| | Name | Angaben zur Identität | Gründe | Datum der Aufnahme in die Liste |
|---|---|---|---|---|
| | | | 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.<br>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. | |
| 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.<br>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.<br>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.<br>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 |

▼M2

| | Name | Angaben zur Identität | Gründe | Datum der Aufnahme in die Liste |
|---|---|---|---|---|
| ▼M13 | | | | |
| 5. | Integrity Technology Group | 永信至诚科技集团股份有限公司<br>(chinesische Schreibweise)<br>Aliasname:<br>Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited<br>Adresse: Fenghao East Road, Room 103, Building 6, No. 9, Beijing Haidian District, China<br>Ort der Registrierung: Peking, China<br>Registrierungsdatum: 2.9.2010<br>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.<br>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 |
| 6. | Emennet Pasargad | Aliasname:<br>Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten<br>Ort der Registrierung: Teheran, Iran<br>Registrierungsnummer: 554267<br>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.<br>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. | 16.3.2026 |

▼M13

| | Name | Angaben zur Identität | Gründe | Datum der Aufnahme in die Liste |
|---|---|---|---|---|
| | | | 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. | |
| 7. | Anxun Information Technology Co. Ltd. | 安洵信息技术有限公司<br>(chinesische Schreibweise)<br>Aliasname: i-Soon<br>Adresse: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai<br>Unified Social Credit Code (Chinesische Steuernummer): 91510105332025597A (Zweigniederlassung Sichuan)<br>Unified Social Credit Code (Chinesische Steuernummer): 91310116561906136G (Zweigniederlassung Shanghai)<br>Website: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win<br>Telefonnummern: +862161119992, +8605645893417, +8613761671735, +864000665915<br>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.<br>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 |