2024/1391

17.5.2024

DECYZJA RADY (WPZIB) 2024/1391

z dnia 17 maja 2024 r.

zmieniająca decyzję (WPZiB) 2019/797 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o Unii Europejskiej, w szczególności jego art. 29,

uwzględniając wniosek Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa,

a także mając na uwadze, co następuje:

(1) W dniu 17 maja 2019 r. Rada przyjęła decyzję (WPZiB) 2019/797 ([1]).

(2) Decyzję (WPZiB) 2019/797 stosuje się do 18 maja 2025 r. Z przeglądu tej decyzji wynika, że obowiązywanie określonych w niej środków ograniczających należy przedłużyć do tego dnia.

(3) Ze względu na nieustanne i coraz liczniejsze szkodliwe działania w cyberprzestrzeni, w tym działania wymierzone w państwa trzecie, należy zaktualizować powody włączenia w przypadku sześciu osób i dwóch podmiotów do wykazu osób fizycznych i prawnych, podmiotów i organów objętych sankcjami zamieszczonego w załączniku do decyzji (WPZiB) 2019/797.

(4) Należy zatem odpowiednio zmienić decyzję (WPZiB) 2019/797,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

W decyzji (WPZiB) 2019/797 wprowadza się następujące zmiany:

1) art. 10 otrzymuje brzmienie:

„*Artykuł 10*

Niniejszą decyzję stosuje się do dnia 18 maja 2025 r. Jest ona poddawana stałemu przeglądowi.”;

2) w załączniku wprowadza się zmiany zgodnie z załącznikiem do niniejszej decyzji.

Artykuł 2

Niniejsza decyzja wchodzi w życie następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono w Brukseli dnia 17 maja 2024 r.

W imieniu Rady

Przewodnicząca

H. LAHBIB

([1]) Decyzja Rady (WPZiB) 2019/797 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim (Dz.U. L 129 I z 17.5.2019, s. 13).

ZAŁĄCZNIK

W załączniku do decyzji (WPZiB) 2019/797 („Wykaz osób fizycznych i prawnych, podmiotów i organów, o których mowa w art. 4 i 5”) wprowadza się następujące zmiany:

1) w wykazie zatytułowanym „A. Osoby fizyczne”, wpisy 3–8 otrzymują brzmienie:

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
„3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Data urodzenia: 27.5.1972 Miejsce urodzenia: obwód permski, Rosyjska FSRR (obecnie Federacja Rosyjska) Numer paszportu: 120017582 Wydany przez: Ministerstwo Spraw Zagranicznych Federacji Rosyjskiej Okres ważności: od 17 kwietnia 2017 r. do 17 kwietnia 2022 r. Miejsce: Moskwa, Federacja Rosyjska Obywatelstwo: rosyjskie Płeć: mężczyzna	Alexey Minin wziął udział w próbie cyberataku na Organizację ds. Zakazu Broni Chemicznej (OPCW) w Niderlandach, który mógł wywołać poważne skutki, oraz w cyberatakach na państwa trzecie o poważnych skutkach. Jako oficer wsparcia wywiadu osobowego Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GU GRU) Alexey Minin należał do zespołu czterech rosyjskich oficerów wywiadu wojskowego, którzy w kwietniu 2018 r. dokonali próby uzyskania nieuprawnionego dostępu do sieci Wi-Fi OPCW w Hadze w Niderlandach. Próba cyberataku miała na celu włamanie się do sieci Wi-Fi OPCW; gdyby atak ten się powiódł, zagroziłby bezpieczeństwu sieci i pracom dochodzeniowym prowadzonym przez OPCW. Wywiad Wojskowy i Służby Bezpieczeństwa Niderlandów (Militaire Inlichtingen- en Veiligheidsdienst) przerwały tę próbę cyberataku, uniemożliwiając w ten sposób wyrządzenie poważnej szkody OPCW. Alexey Minin jako oficer rosyjskiego Głównego Zarządu Wywiadowczego (GRU) został przez wielką ławę przysięgłych w Sądzie Okręgowym dla Okręgu Zachodniego w Pensylwanii (Stany Zjednoczone) uznany za winnego hakerstwa, internetowych oszustw finansowych, kwalifikowanej kradzieży tożsamości i prania pieniędzy.	30.7.2020

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

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Data urodzenia: 31.7.1977 Miejsce urodzenia: obwód murmański, Rosyjska FSRR (obecnie Federacja Rosyjska) Numer paszportu: 100135556 Wydany przez: Ministerstwo Spraw Zagranicznych Federacji Rosyjskiej Okres ważności: od 17 kwietnia 2017 r. do 17 kwietnia 2022 r. Miejsce: Moskwa, Federacja Rosyjska Obywatelstwo: rosyjskie Płeć: mężczyzna	Aleksei Morenets wziął udział w próbie cyberataku na Organizację ds. Zakazu Broni Chemicznej (OPCW) w Niderlandach, który mógł wywołać poważne skutki, oraz w cyberatakach na państwa trzecie o poważnych skutkach. Jako cyberoperator Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GU GRU) Aleksei Morenets należał do zespołu czterech rosyjskich oficerów wywiadu wojskowego, którzy w kwietniu 2018 r. dokonali próby uzyskania nieuprawnionego dostępu do sieci Wi-Fi OPCW w Hadze w Niderlandach. Próba cyberataku miała na celu włamanie się do sieci Wi-Fi OPCW; gdyby atak ten się powiódł, zagroziłby bezpieczeństwu sieci i pracom dochodzeniowym prowadzonym przez OPCW. Wywiad Wojskowy i Służby Bezpieczeństwa Niderlandów (Militaire Inlichtingen- en Veiligheidsdienst) przerwały tę próbę cyberataku, uniemożliwiając w ten sposób wyrządzenie poważnej szkody OPCW. Aleksei Morenetes jako członek jednostki wojskowej 26165 został przez wielką ławę przysięgłych w Sądzie Okręgowym dla Okręgu Zachodniego w Pensylwanii (Stany Zjednoczone) uznany za winnego hakerstwa, internetowych oszustw finansowych, kwalifikowanej kradzieży tożsamości i prania pieniędzy.	30.7.2020

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Data urodzenia: 26.7.1981 Miejsce urodzenia: Kursk, Rosyjska FSRR (obecnie Federacja Rosyjska) Numer paszportu: 100135555 Wydany przez: Ministerstwo Spraw Zagranicznych Federacji Rosyjskiej Okres ważności: od 17 kwietnia 2017 r. do 17 kwietnia 2022 r. Miejsce: Moskwa, Federacja Rosyjska Obywatelstwo: rosyjskie Płeć: mężczyzna	Evgenii Serebriakov wziął udział w próbie cyberataku na Organizację ds. Zakazu Broni Chemicznej (OPCW) w Niderlandach, który mógł wywołać poważne skutki, oraz w cyberatakach na państwa trzecie o poważnych skutkach. Jako cyberoperator Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GU GRU) Evgenii Serebriakov należał do zespołu czterech rosyjskich oficerów wywiadu wojskowego, którzy w kwietniu 2018 r. dokonali próby uzyskania nieuprawnionego dostępu do sieci Wi-Fi OPCW w Hadze w Niderlandach. Próba cyberataku miała na celu włamanie się do sieci Wi-Fi OPCW; gdyby atak ten się powiódł, zagroziłby bezpieczeństwu sieci i pracom dochodzeniowym prowadzonym przez OPCW. Wywiad Wojskowy i Służby Bezpieczeństwa Niderlandów (Militaire Inlichtingen- en Veiligheidsdienst) przerwały tę próbę cyberataku, uniemożliwiając w ten sposób wyrządzenie poważnej szkody OPCW. Od wiosny 2022 r. Evgenii Serebriakov stoi na czele zajmującej się wojną cybernetyczną grupy hakerów »Sandworm« (inne nazwy: »Sandworm Team«, »BlackEnergy Group«, »Voodoo Bear«, »Quedagh«, »Olympic Destroyer« i »Telebots«) powiązanej z jednostką 74455 rosyjskiego Głównego Zarządu Wywiadowczego. Sandworm przeprowadziła cyberataki na Ukrainę, w tym ukraińskie agencje rządowe, w związku z rosyjską wojną napastniczą przeciwko Ukrainie.	30.7.2020

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Data urodzenia: 24.8.1972 Miejsce urodzenia: Uljanowsk, Rosyjska FSRR (obecnie Federacja Rosyjska) Numer paszportu: 120018866 Wydany przez: Ministerstwo Spraw Zagranicznych Federacji Rosyjskiej Okres ważności: od 17 kwietnia 2017 r. do 17 kwietnia 2022 r. Miejsce: Moskwa, Federacja Rosyjska Obywatelstwo: rosyjskie Płeć: mężczyzna	Oleg Sotnikov wziął udział w próbie cyberataku na Organizację ds. Zakazu Broni Chemicznej (OPCW) w Niderlandach, który mógł wywołać poważne skutki, oraz w cyberatakach na państwa trzecie o poważnych skutkach. Jako oficer wsparcia wywiadu osobowego Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GU GRU) Oleg Sotnikov należał do zespołu czterech rosyjskich oficerów wywiadu wojskowego, którzy w kwietniu 2018 r. dokonali próby uzyskania nieuprawnionego dostępu do sieci Wi-Fi OPCW w Hadze w Niderlandach. Próba cyberataku miała na celu włamanie się do sieci Wi-Fi OPCW; gdyby atak ten się powiódł, zagroziłby bezpieczeństwu sieci i pracom dochodzeniowym prowadzonym przez OPCW. Wywiad Wojskowy i Służby Bezpieczeństwa Niderlandów (Militaire Inlichtingen- en Veiligheidsdienst) przerwały tę próbę cyberataku, uniemożliwiając w ten sposób wyrządzenie poważnej szkody OPCW. Oleg Sotnikov jako oficer rosyjskiego Głównego Zarządu Wywiadowczego (GRU) został przez wielką ławę przysięgłych w Sądzie Okręgowym dla Okręgu Zachodniego w Pensylwanii uznany za winnego hakerstwa, internetowych oszustw finansowych, kwalifikowanej kradzieży tożsamości i prania pieniędzy.	30.7.2020

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Data urodzenia: 15.11.1990 Miejsce urodzenia: Kursk, Rosyjska FSRR (obecnie Federacja Rosyjska) Obywatelstwo: rosyjskie Płeć: mężczyzna	Dmitry Badin wziął udział w cyberataku o poważnych skutkach wymierzonym w niemiecki parlament federalny (Deutscher Bundestag) oraz w cyberatakach na państwa trzecie o poważnych skutkach. Dmitry Badin, jako oficer wywiadu wojskowego 85. Głównego Ośrodka Służb Specjalnych (GTsSS) Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GU GRU), był członkiem zespołu rosyjskich oficerów wywiadu wojskowego, którzy przeprowadzili w kwietniu i maju 2015 r. cyberatak wymierzony w niemiecki parlament federalny. Celem tego cyberataku był system informacyjny parlamentu; atak ten miał wpływ na funkcjonowanie tej instytucji przez kilka dni. Skradziono dużą ilość danych; atak ten obejmował także konta poczty elektronicznej kilkorga parlamentarzystów, w tym byłej kanclerz Angeli Merkel. Dmitry Badin jako członek jednostki wojskowej 26165 został przez wielką ławę przysięgłych w Sądzie Okręgowym dla Okręgu Zachodniego w Pensylwanii (Stany Zjednoczone) uznany za winnego hakerstwa, internetowych oszustw finansowych, kwalifikowanej kradzieży tożsamości i prania pieniędzy.	22.10.2020

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Data urodzenia: 21.2.1961 Obywatelstwo: rosyjskie Płeć: mężczyzna	Igor Kostyukow jest obecnie szefem Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GU GRU), gdzie poprzednio sprawował funkcję pierwszego zastępcy szefa. Jednym z oddziałów pod jego dowództwem jest 85. Główny Ośrodek Służb Specjalnych (GTsSS) (alias »jednostka wojskowa 26165«, »APT28«, »Fancy Bear«, »Sofacy Group«, »Pawn Storm« i »Strontium«). Pełniąc tę funkcję, Igor Kostyukow jest odpowiedzialny za cyberataki przeprowadzone przez GTsSS, w tym cyberataki o poważnych skutkach stanowiące zewnętrzne zagrożenie dla Unii lub jej państw członkowskich. W szczególności oficerowie wywiadu wojskowego GTsSS brali udział w cyberataku wymierzonym w niemiecki parlament federalny (Deutscher Bundestag) w kwietniu i maju 2015 r. oraz w próbie cyberataku, którego celem było włamanie do sieci WiFi Organizacji ds. Zakazu Broni Chemicznej (OPCW) w Niderlandach w kwietniu 2018 r. Celem cyberataku wymierzonego w niemiecki parlament federalny był system informacyjny parlamentu; atak ten miał wpływ na funkcjonowanie tej instytucji przez kilka dni. Skradziono dużą ilość danych; atak ten obejmował także konta poczty elektronicznej kilkorga parlamentarzystów, w tym byłej kanclerz Angeli Merkel.	22.10.2020”

2) w wykazie zatytułowanym „B. Osoby prawne, podmioty i organy” wpisy 3 i 4 otrzymują brzmienie:

	Nazwa	Dane identyfikacyjne	Powody	Data umieszczenia
„3.	Główny Ośrodek Specjalnych Technologii (GTsST) Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GU GRU)	Adres: 22 Kirova Street, Moscow, Russian Federation	Główny Ośrodek Specjalnych Technologii (GTsST) Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GU GRU), znany również jako jednostka numer 74455, jest odpowiedzialny za cyberataki o poważnych skutkach, których sprawcy znajdują się poza Unią i które stanowią zewnętrzne zagrożenie dla Unii lub jej państw członkowskich, oraz cyberataki o poważnych skutkach dla państw trzecich, w tym cyberataki powszechnie znane jako »NotPetya« lub »EternalPetya« z czerwca 2017 r. oraz cyberataki wymierzone w ukraińską sieć elektroenergetyczną zimą 2015 i 2016 r. Ataki »NotPetya« lub »EternalPetya« spowodowały brak dostępności danych w wielu przedsiębiorstwach w Unii, szerzej w Europie i na całym świecie poprzez uderzenie w komputery za pomocą oprogramowania szantażującego i zablokowanie dostępu do danych, co doprowadziło między innymi do znacznych strat gospodarczych. Cyberatak na ukraińską sieć elektroenergetyczną spowodował wyłączenie jej części zimą. Ataki »NotPetya« lub »EternalPetya« zostały przeprowadzone przez grupę powszechnie znaną jako »Sandworm« (inne nazwy: »Sandworm Team«, »BlackEnergy Group«, »Voodoo Bear«, »Quedagh«, »Olympic Destroyer« i »Telebots«), która stoi również za atakiem na ukraińską sieć elektroenergetyczną. Grupa ta przeprowadziła cyberataki na Ukrainę, w tym ukraińskie agencje rządowe i ukraińską infrastrukturę krytyczną, w związku z rosyjską wojną napastniczą przeciwko Ukrainie. Cyberataki te obejmowały kampanie profilowanego phishingu (*spear-phishing*) oraz ataki przy użyciu złośliwego i szantażującego oprogramowania. Główny Ośrodek Specjalnych Technologii Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej odgrywa czynną rolę w działaniach w cyberprzestrzeni podejmowanych przez grupę »Sandworm« i może zostać powiązany z tą grupą.	30.7.2020

	Nazwa	Dane identyfikacyjne	Powody	Data umieszczenia
4.	Główny Ośrodek Służb Specjalnych (GTsSS) Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GU GRU)	Adres: Adres: Komsomol'skiy Prospekt, 20, Moscow, 119146, Russian Federation	85. Główny Ośrodek Służb Specjalnych (GTsSS) Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GU GRU) (alias »jednostka wojskowa 26165«, »APT28«, »Fancy Bear«, »Sofacy Group«, »Pawn Storm« i »Strontium«), jest odpowiedzialny za cyberataki o poważnych skutkach stanowiące zewnętrzne zagrożenie dla Unii lub jej państw członkowskich oraz za cyberataki na państwa trzecie o poważnych skutkach. W szczególności oficerowie wywiadu wojskowego GTsSS brali udział w cyberataku wymierzonym w niemiecki parlament federalny (Deutscher Bundestag) w kwietniu i maju 2015 r. oraz w próbie cyberataku, którego celem było włamanie do sieci Wi-Fi Organizacji ds. Zakazu Broni Chemicznej (OPCW) w Niderlandach w kwietniu 2018 r. Celem cyberataku wymierzonego w niemiecki parlament federalny był system informacyjny parlamentu; atak ten miał wpływ na funkcjonowanie tej instytucji przez kilka dni. Skradziono dużą ilość danych; atak ten obejmował także konta poczty elektronicznej kilkorga parlamentarzystów, w tym byłej kanclerz Angeli Merkel. W związku z rosyjską wojną napastniczą przeciwko Ukrainie GTsSS przeprowadził cyberataki na Ukrainę (przy użyciu profilowanego phishingu i złośliwego oprogramowania).	22.10.2020”