Rada
Evropské unie

Brusel 13. května 2024
(OR. en)

8500/24

LIMITE

CORLX 354
CFSP/PESC 510
CYBER 108
JAI 570
FIN 339

PRÁVNÍ PŘEDPISY A JINÉ AKTY

Předmět:	ROZHODNUTÍ RADY, kterým se mění rozhodnutí (SZBP) 2019/797 o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy

ROZHODNUTÍ RADY (SZBP) 2024/…

ze dne ...,

kterým se mění rozhodnutí (SZBP) 2019/797 o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy

RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o Evropské unii, a zejména na článek 29 této smlouvy,

s ohledem na návrh vysokého představitele Unie pro zahraniční věci a bezpečnostní politiku,

vzhledem k těmto důvodům:

(1) Dne 17. května 2019 přijala Rada rozhodnutí (SZBP) 2019/797[1].

(2) Rozhodnutí (SZBP) 2019/797 je použitelné do 18. května 2025. Na základě přezkumu uvedeného rozhodnutí by platnost omezujících opatření v něm obsažených měla být prodloužena do uvedeného data.

(3) Vzhledem k pokračujícím a stále intenzivnějším nepřátelským činnostem v kyberprostoru, včetně činností namířených proti třetím státům, by měla být aktualizována odůvodnění pro zařazení šesti osob a dvou subjektů na seznam fyzických a právnických osob, subjektů a orgánů, na něž se vztahují omezující opatření, stanovený v příloze rozhodnutí (SZBP) 2019/797.

(4) Rozhodnutí (SZBP) 2019/797 by proto mělo být odpovídajícím způsobem změněno,

PŘIJALA TOTO ROZHODNUTÍ:

[1] Rozhodnutí Rady (SZBP) 2019/797 ze dne 17. května 2019 o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy (Úř. věst. L 129I, 17.5.2019, s. 13).

Článek 1

Rozhodnutí (SZBP) 2019/797 se mění takto:

1) Článek 10 se nahrazuje tímto:

„*Článek 10*

Toto rozhodnutí se použije do 18. května 2025 a je průběžně přezkoumáváno.“;

2) Příloha se mění v souladu s přílohou tohoto rozhodnutí.

Článek 2

Toto rozhodnutí vstupuje v platnost prvním dnem po vyhlášení v *Úředním věstníku Evropské unie*.

V ... dne ...

Za Radu
předseda/předsedkyně

PŘÍLOHA

Příloha rozhodnutí (SZBP) 2019/797 („Seznam fyzických a právnických osob, subjektů a orgánů podle článků 4 a 5“) se mění takto:

1) V seznamu v oddíle „A. Fyzické osoby“ se položky 3 až 8 nahrazují tímto:

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
„3.	Alexey Valeryevich MININ (Alexej Valerjevič Minin)	Алексей Валерьевич МИНИН Datum narození: 27.5.1972 Místo narození: Permská oblast, Ruská SFSR (nyní Ruská federace) Číslo pasu: 120017582 Vydalo: Ministerstvo zahraničních věcí Ruské federace Platnost: od 17.4.2017 do 17.4.2022 Místo výkonu zaměstnání: Moskva, Ruská federace Státní příslušnost: ruská Pohlaví: muž	Alexej Minin se podílel na pokusu o kybernetický útok s potenciálně významným dopadem na Organizaci pro zákaz chemických zbraní (OPCW) v Nizozemsku a na kybernetických útocích s významným dopadem na třetí státy. Jako důstojník pro podporu zpravodajství lidských zdrojů působící v rámci hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU) byl Alexej Minin součástí týmu čtyř ruských vojenských zpravodajských důstojníků, kteří se v dubnu 2018 pokusili získat neoprávněný přístup do bezdrátové sítě organizace OPCW v Haagu (Nizozemsko). Pokus o kybernetický útok byl zaměřen na proniknutí do bezdrátové sítě organizace OPCW, který by v případě úspěchu ohrozil bezpečnost sítě a probíhající vyšetřovací činnost této organizace. Nizozemská obranná zpravodajská a bezpečnostní služba (Militaire Inlichtingen- en Veiligheidsdienst) pokus o kybernetický útok zmařila, čímž zabránila vážným škodám pro organizaci OPCW. Velká porota Západního okresu Pensylvánie (Spojené státy americké) obvinila Alexeje Minina, jako důstojníka hlavního ředitelství ruské zpravodajské služby (GRU), z hackerských útoků, podvodů prostřednictvím elektronické komunikace, krádeží totožnosti s přitěžujícími okolnostmi a praní špinavých peněz.	30.7.2020

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
4.	Aleksei Sergeyvich MORENETS (Alexej Sergejevič Moreněc)	Алексей Сергеевич МОРЕНЕЦ Datum narození: 31.7.1977 Místo narození: Murmanská oblast, Ruská SFSR (nyní Ruská federace) Číslo pasu: 100135556 Vydalo: Ministerstvo zahraničních věcí Ruské federace Platnost: od 17.4.2017 do 17.4.2022 Místo výkonu zaměstnání: Moskva, Ruská federace Státní příslušnost: ruská Pohlaví: muž	Alexej Moreněc se podílel na pokusu o kybernetický útok s potenciálně významným dopadem na Organizaci pro zákaz chemických zbraní (OPCW) v Nizozemsku a na kybernetických útocích s významným dopadem na třetí státy. Jako pracovník pro kybernetické operace působící v rámci hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU) byl Alexej Moreněc součástí týmu čtyř ruských vojenských zpravodajských důstojníků, kteří se v dubnu 2018 pokusili získat neoprávněný přístup do bezdrátové sítě organizace OPCW v Haagu (Nizozemsko). Pokus o kybernetický útok byl zaměřen na proniknutí do bezdrátové sítě organizace OPCW, který by v případě úspěchu ohrozil bezpečnost sítě a probíhající vyšetřovací činnost této organizace. Nizozemská obranná zpravodajská a bezpečnostní služba (Militaire Inlichtingen- en Veiligheidsdienst) pokus o kybernetický útok zmařila, čímž zabránila vážným škodám pro organizaci OPCW. Velká porota Západního okresu Pensylvánie (Spojené státy americké) obvinila Alexeje Moreněce, přiděleného k vojenské jednotce 26165, z hackerských útoků, podvodů prostřednictvím elektronické komunikace, krádeží totožnosti s přitěžujícími okolnostmi a praní špinavých peněz.	30.7.2020

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
5.	Evgenii Mikhaylovich SEREBRIAKOV (Jevgenij Michailovič Serebrjakov)	Евгений Михайлович СЕРЕБРЯКОВ Datum narození: 26.7.1981 Místo narození: Kursk, Ruská SFSR (nyní Ruská federace) Číslo pasu: 100135555 Vydalo: Ministerstvo zahraničních věcí Ruské federace. Platnost: od 17.4.2017 do 17.4.2022 Místo: Moskva, Ruská federace Státní příslušnost: ruská Pohlaví: muž	Jevgenij Serebrjakov se podílel na pokusu o kybernetický útok s potenciálně významným dopadem na Organizaci pro zákaz chemických zbraní (OPCW) v Nizozemsku a na kybernetických útocích s významným dopadem na třetí státy. Jako pracovník pro kybernetické operace působící v rámci hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU) byl Jevgenij Serebrjakov součástí týmu čtyř ruských vojenských zpravodajských důstojníků, kteří se v dubnu 2018 pokusili získat neoprávněný přístup do bezdrátové sítě organizace OPCW v Haagu (Nizozemsko). Pokus o kybernetický útok byl zaměřen na proniknutí do bezdrátové sítě organizace OPCW, který by v případě úspěchu ohrozil bezpečnost sítě a probíhající vyšetřovací činnost této organizace. Nizozemská obranná zpravodajská a bezpečnostní služba (Militaire Inlichtingen- en Veiligheidsdienst) pokus o kybernetický útok zmařila, čímž zabránila vážným škodám pro organizaci OPCW. Od jara 2022 vede Jevgenij Serebrjakov aktéra a hackerskou skupinu „Sandworm“ (také známa jako „Sandworm Team“, „BlackEnergy Group“, „Voodoo Bear“, „Quedagh“, „Olympic Destroyer“ a „Telebots“), přidruženou k jednotce 74455 hlavního ředitelství ruské zpravodajské služby. V kontextu útočné války Ruska proti Ukrajině provádí Sandworm kybernetické útoky zaměřené na Ukrajinu, včetně ukrajinských vládních orgánů.	30.7.2020

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
6.	Oleg Mikhaylovich SOTNIKOV (Oleg Michajlovič Sotnikov)	Олег Михайлович СОТНИКОВ Datum narození: 24.8.1972 Místo narození: Uljanovsk, Ruská SFSR (nyní Ruská federace) Číslo pasu: 120018866 Vydalo: Ministerstvo zahraničních věcí Ruské federace Platnost: od 17.4.2017 do 17. 4.2022 Místo výkonu zaměstnání: Moskva, Ruská federace Státní příslušnost: ruská Pohlaví: muž	Oleg Sotnikov se podílel na pokusu o kybernetický útok s potenciálně významným dopadem na Organizaci pro zákaz chemických zbraní (OPCW) v Nizozemsku a na kybernetických útocích s významným dopadem na třetí státy. Jako důstojník pro podporu zpravodajství lidských zdrojů působící v rámci hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU) byl Oleg Sotnikov součástí týmu čtyř ruských vojenských zpravodajských důstojníků, kteří se v dubnu 2018 pokusili získat neoprávněný přístup do bezdrátové sítě organizace OPCW v Haagu (Nizozemsko). Pokus o kybernetický útok byl zaměřen na proniknutí do bezdrátové sítě organizace OPCW, který by v případě úspěchu ohrozil bezpečnost sítě a probíhající vyšetřovací činnost této organizace. Nizozemská obranná zpravodajská a bezpečnostní služba (Militaire Inlichtingen- en Veiligheidsdienst) pokus o kybernetický útok zmařila, čímž zabránila vážným škodám pro organizaci OPCW. Velká porota Západního okresu Pensylvánie obvinila Olega Sotnikova, jako důstojníka hlavního ředitelství ruské zpravodajské služby (GRU), z hackerských útoků, podvodů prostřednictvím elektronické komunikace, krádeží totožnosti s přitěžujícími okolnostmi a praní špinavých peněz.	30.7.2020

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
7.	Dmitry Sergeyevich BADIN (Dmitrij Sergejevič Badin)	Дмитрий Сергеевич БАДИН Datum narození: 15.11.1990 Místo narození: Kursk, Ruská SFSR (nyní Ruská federace) Státní příslušnost: ruská Pohlaví: muž	Dmitrij Badin se podílel na kybernetickém útoku s významným dopadem namířeném proti německému Spolkovému sněmu (Deutscher Bundestag) a na kybernetických útocích s významným dopadem na třetí státy. Jako vojenský zpravodajský důstojník 85. hlavního střediska pro speciální služby (GTsSS) hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU) byl Dmitrij Badin součástí týmu ruských vojenských zpravodajských důstojníků, kteří v dubnu a květnu 2015 provedli kybernetický útok na německý Spolkový sněm. Uvedený kybernetický útok byl namířen proti informačnímu systému sněmu a na několik dní narušil jeho provoz. Byl při něm odcizen značný objem dat a byly postiženy emailové účty několika poslanců, jakož i bývalé kancléřky Angely Merkelové. Velká porota Západního okresu Pensylvánie (Spojené státy americké) obvinila Dmitrije Badina, přiděleného k vojenské jednotce 26165, z hackerských útoků, podvodů prostřednictvím elektronické komunikace, krádeží totožnosti s přitěžujícími okolnostmi a praní špinavých peněz.	22.10.2020

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
8.	Igor Olegovich KOSTYUKOV (Igos Olegovič Kosťukov)	Игорь Олегович КОСТЮКОВ Datum narození: 21.2.1961 Státní příslušnost: ruská Pohlaví: muž	Igor Kosťukov je v současné době vedoucím hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU), kde předtím působil jako první náměstek vedoucího. Jedním z oddělení, která spadají pod jeho vedení, je 85. hlavní středisko pro speciální služby (GTsSS) (také známé jako „vojenská jednotka 26165“ „APT28“, „Fancy Bear“, „Sofacy Group“, „Pawn Storm“ a „Strontium“). Ze své funkce je Igor Kosťukov odpovědný za kybernetické útoky provedené GTsSS, včetně kybernetických útoků s významným dopadem, které představují vnější hrozbu pro Unii nebo její členské státy. Vojenští zpravodajští důstojníci GTsSS se zejména podíleli na kybernetickém útoku na německý Spolkový sněm (Deutscher Bundestag) v dubnu a květnu 2015, a na pokusu o kybernetický útok, k němuž došlo v dubnu 2018, jehož cílem bylo proniknout do bezdrátové sítě Organizace pro zákaz chemických zbraní (OPCW) v Nizozemsku. Kybernetický útok na německý Spolkový sněm byl namířen proti informačnímu systému sněmu a na několik dní narušil jeho provoz. Byl při něm odcizen značný objem dat a byly postiženy emailové účty několika poslanců, jakož i bývalé kancléřky Angely Merkelové.	22.10.2020“

2) V seznamu v oddíle „B. Právnické osoby, subjekty a orgány“ se položky 3 a 4 nahrazují tímto:

	Název	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
„3.	Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) (Hlavní středisko pro speciální technologie (GTsST) hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU))	Adresa: Ul. Kirova 22, Moskva, Ruská federace	Hlavní středisko pro speciální technologie (GTsST) hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU), známé rovněž pod svým systémovým identifikačním číslem 74455, je zapojeno do kybernetických útoků s významným dopadem pocházejících ze zemí mimo Unii a představujících vnější hrozbu pro Unii nebo její členské státy a do kybernetických útoků s významným dopadem na třetí státy, včetně kybernetických útoků veřejně známých jako „NotPetya“ nebo „EternalPetya“ provedených v červnu 2017 a kybernetických útoků namířených na ukrajinskou elektrickou rozvodnou síť v zimě 2015 a 2016. Kybernetické útoky „NotPetya“ nebo „EternalPetya“ znemožnily přístup k údajům v řadě společností v Unii, v širší Evropě a po celém světě tím, že se zaměřily na počítače pomocí ransomwaru a zablokovaly přístup k údajům, což mělo mimo jiné za následek významné ekonomické ztráty. Kybernetický útok na ukrajinskou elektrickou rozvodnou síť způsobil, že její části byly během zimy odpojeny.	30.7.2020

	Název	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
			Za útokem na ukrajinskou elektrickou síť, který byl proveden pomocí útoků „NotPetya“ nebo „EternalPetya“, stál aktér veřejně známý jako „Sandworm“ (také znám jako „Sandworm Team“, „BlackEnergy Group“, „Voodoo Bear“, „Quedagh“, „Olympic Destroyer“ a „Telebots“). V kontextu útočné války Ruska proti Ukrajině provádí Sandworm kybernetické útoky na Ukrajinu, včetně ukrajinských vládních orgánů a ukrajinské kritické infrastruktury. Mezi tyto kybernetické útoky patří spearphishingové kampaně, malwarové a ransomwarové útoky. Hlavní středisko pro speciální technologie hlavního ředitelství generálního štábu ozbrojených sil Ruské federace se aktivně podílí na kybernetických činnostech prováděných aktérem Sandworm a může být na tohoto aktéra napojeno.	

	Název	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
4.	85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) (85. hlavní středisko pro speciální služby (GTsSS) hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU))	Adresa: Komsomolskij Prospekt, 20, Moskva, 119146, Ruská federace	85. hlavní středisko pro speciální služby (GTsSS) hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU)) (také známé jako „vojenská jednotka 26165“„APT28“, „Fancy Bear“, „Sofacy Group“, „Pawn Storm“ a „Strontium“) je zapojeno do kybernetických útoků s významným dopadem, které představují vnější hrozbu pro Unii nebo její členské státy, a do kybernetických útoků s významným dopadem na třetí státy. Vojenští zpravodajští důstojníci GTsSS se zejména podíleli na kybernetickém útoku na německý Spolkový sněm (Deutscher Bundestag) v dubnu a květnu 2015, a na pokusu o kybernetický útok v dubnu 2018, jehož cílem bylo proniknout do bezdrátové sítě Organizace pro zákaz chemických zbraní (OPCW) v Nizozemsku. Kybernetický útok na německý Spolkový sněm byl namířen proti informačnímu systému sněmu a na několik dní narušil jeho provoz. Byl při něm odcizen značný objem dat a byly postiženy emailové účty několika poslanců, jakož i bývalé kancléřky Angely Merkelové. V kontextu útočné války Ruska proti Ukrajině byly ze strany GTsSS proti Ukrajině provedeny kybernetické útoky (spearphishing a malwarové útoky).	22.10.2020“