2026/588

16.3.2026

ROZHODNUTÍ RADY (SZBP) 2026/588

ze dne 16. března 2026,

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 vysoké představitelky Unie pro zahraniční věci a bezpečnostní politiku,

vzhledem k těmto důvodům:

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

(2) V rámci soustavných, individualizovaných a koordinovaných opatření Unie zaměřených proti aktérům přetrvávajících kybernetických hrozeb by na seznam fyzických a právnických osob, subjektů a orgánů, na něž se vztahují omezující opatření, obsažený v příloze rozhodnutí (SZBP) 2019/797, měly být zařazeny dvě fyzické osoby a tři subjekty. Tyto osoby a subjekty jsou odpovědné za kybernetické útoky s významným dopadem, které představují vnější hrozbu pro Unii nebo její členské státy, nebo jsou do těchto útoků zapojeny.

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

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

Příloha rozhodnutí (SZBP) 2019/797 se mění v souladu s přílohou tohoto rozhodnutí.

Článek 2

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

V Bruselu dne 16. března 2026.

Za Radu

předsedkyně

K. KALLAS

([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 129 I, 17.5.2019, s. 13, ELI: http://data.europa.eu/eli/dec/2019/797/oj).

PŘÍLOHA

Příloha rozhodnutí (SZBP) 2019/797 se mění takto:

1) V oddíle „A. Fyzické osoby“ se doplňují nové položky, které znějí:

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
„18.	CHEN Cheng	陈诚 (v čínštině) Také znám jako: Jesse Chen lengmo l3n6m0 Datum narození: 20.10.1984 Místo narození: Yancheng, provincie Tiang-su, Čína Státní příslušnost: čínská Pohlaví: muž	Chen Cheng je čínský podnikatel, spoluzakladatel a jeden z generálních ředitelů (Chief Operating Officer) společnosti Anxun Information Technology Co. Ltd. Je rovněž právním zástupcem pobočky této společnosti v provincii Sečuán. Společnost Anxun Information Technology Co. Ltd., také známá jako i-Soon, je společnost se sídlem v Čínské lidové republice (ČLR), která nabízí služby ‚hacking-for-hire‘ (hacking k pronájmu). Své útoky zaměřila společnost Anxun Information Technology Co. Ltd. na kritickou infrastrukturu a kritické funkce státu v členských státech a získala přístup k utajovaným informacím a prodala je. Společnost Anxun Information Technology Co. Ltd. navíc zaútočila na státní orgány různých třetích států a tím ohrozila cíle společné zahraniční a bezpečnostní politiky (SZBP) Unie stanovené v čl. 21 odst. 2 písm. a) až c) Smlouvy o Evropské unii. Společnost Anxun Information Technology Co. Ltd. získává z poskytovaných služeb významný hospodářský prospěch. Společnost Anxun Information Technology Co. Ltd. je proto odpovědná za kybernetické útoky s významným dopadem, které představují vnější hrozbu pro Unii a její členské státy, jakož i za útoky s na třetí státy. Z titulu své funkce je Chen Cheng odpovědný za kybernetické útoky s významným dopadem, které představují vnější hrozbu pro členské státy, jakož i za kybernetické útoky s významným dopadem na třetí státy a je do těchto útoků zapojen.	16.3.2026

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
19.	WU Haibo	吴海波 (v čínštině) Také znám jako: shutdown shutd0wn Místo narození: Čína Státní příslušnost: čínská Pohlaví: muž	Wu Haibo je čínský podnikatel, spoluzakladatel a jeden z generálních ředitelů (Chief Executive Officer) společnosti Anxun Information Technology Co. Ltd. Je rovněž právním zástupcem, předsedou představenstva a generálním ředitelem pobočky společnosti Anxun Information Technology Co. Ltd. v Šanghaji („mateřské společnosti'). Kromě totho jedná jako právní zástupce pobočky v provincii Sečuán. Společnost Anxun Information Technology Co. Ltd., také známá jako i-Soon, je společnost se sídlem v čínské lidové republice (ČLR), která nabízí služby ‚hacking-for-hire' (hacking k pronájmu). Své útoky zaměřila společnost Anxun Information Technology Co. Ltd na kritickou infrastrukturu a kritické funkce státu v členských státech a získala přístup k utajovaným informacím a prodala je. Společnost Anxun Information Technology Co. Ltd. navíc zaútočila na státní orgány různých třetích států a ohrozila cíle společné zahraniční a bezpečnostní politiky (SZBP) Unie stanovené v čl. 21 odst. 2 písm. a) až c) Smlouvy o Evropské unii. Společnost Anxun Information Technology Co. Ltd. získává z poskytovaných služeb významný hospodářský prospěch. Společnost Anxun Information Technology Co. Ltd. je tudíž odpovědná za kybernetické útoky s významným dopadem, které představují vnější hrozbu pro členské státy, jakož i za útoky na třetí státy. Wu Haibo se podílel na řízení kybernetických útoků s významným dopadem na členské státy a na podněcování pokusů o tyto útoky. Z titulu své funkce je odpovědný za kybernetické útoky s významným dopadem, které představují vnější hrozbu pro členské státy, jakož i za kybernetické útoky s významným dopadem na třetí státy a je do těchto útoků zapojen..	16.3.2026“

2) V oddíle „B. Právnické osoby, subjekty a orgány“ se doplňují nové položky, které znějí:

	Název	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
„5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (v čínštině) Také známa jako: Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited Adresa: Fenghao East Road, Room 103, Building 6, No. 9, Beijing Haidian District, Čína Místo registrace: Peking, Čína Datum registrace: 2.9.2010 Unified social credit code (čínské registrační číslo): 91110108562135265P	Společnost Integrity Technology Group je podnik působící v oblasti kybernetické bezpečnosti se sídlem v Čínské lidové republice (ČLR), který usnadňoval kybernetické útoky spojené se skupinou Flax Typhoon, která je aktérem pokročilé trvalé hrozby (APT). Tato APT využívala k realizaci svých činností v oblasti využívání počítačových sítí produkty a technologie společnosti Integrity Technology Group. Produkty společnosti Integrity Technology Group se od té doby používají ke kompromitaci zařízení v rámci internetu věcí v členských státech, v dalších evropských zemích i na celosvětové úrovni a k získání přístupu k těmto zařízením. V letech 2022 až 2023 získala Flax T pomocí produktů společnosti Integrity Technology Group přístup k nejméně 65 600 zařízení v rámci internetu věcí v šesti členských státech. Komerční produkty a infrastruktura společnosti Integrity Technology Group byly proto běžně využívány při kybernetických útocích proti členským i třetím státům. Tím, že Integrity Technology Group ovlivňuje informační systémy týkající se digitální infrastruktury, poskytuje tudíž tato společnost technickou a materiální podporu pro kybernetické útoky s významným dopadem, které představují vnější hrozbu pro členské a třetí státy.	16.3.2026

	Název	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
6.	Emennet Pasargad	Také známa jako: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten Místo registrace: Teherán, Írán Registrační číslo: 554267 Hlavní místo obchodní činnosti: Teherán, Írán	Společnost Emennet Pasargad je íránský kybernetický aktér (společnost), který své útoky zaměřil na řadu subjektů, zejména v členských státech, jakož i ve Spojených státech (USA). Společnost Emennet Pasargard, působící pod názvem ‚Anzu Team', zaměřila své útoky na digitální infrastrukturu ve Švédsku a kompromitovala švédskou službu pro zasílání SMS zpráv, což mělo nepříznivý dopad na velký počet osob. Kromě toho tento subjekt, který jednal pod názvem ‚Holy Souls', kompromitoval databázi předplatitelů francouzského satirického časopisu Charlie Hebdo a na temném webu ji inzeroval k prodeji. Společnost Emennet Pasargard během olympijských her v Paříži kompromitovala reklamní billboardy a zobrazila na nich pozměněný obsah v rámci dezinformačních kampaní. Společnost Emennet Pasargard se rovněž pokusila zasáhnout do prezidentských voleb v USA v roce 2020, přičemž ohrozila demokracii a právní stát tím, že získala důvěrné informace o voličích v USA a neoprávněný přístup k počítačové síti jedné z amerických mediálních společností. Společnost Emennet Pasargard je tudíž odpovědná za kybernetické útoky s významným dopadem, které představují vnější hrozbu pro členské státy, a za kybernetické útoky s významným dopadem na třetí státy.	16.3.2026

	Název	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
7.	Anxun Information Technology Co. Ltd	安洵信息技术有限公司 (v čínštině) Také známa jako: i-Soon Adresa: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Šanghaj Unified social credit code (čínské registrační číslo): 91510105332025597A (pobočka v provincii Sečuán) Unified social credit code (čínské registrační číslo): 91310116561906136G (pobočka v Šanghaji) Internetové stránky: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win Telefonní čísla: +862161119992, +8605645893417, +8613761671735, +864000665915 E-mailové adresy: shutdown@163.com, isoon2015@126.com, tao_tingting@i-soon.net, li_ping@i-soon.net	Společnost Anxun Information Technology Co. Ltd. je společnost se sídlem v Čínské lidové republice, která nabízí služby ‚hacking-for-hire' (hacking k pronájmu). Své útoky zaměřila na kritickou infrastrukturu a kritické funkce státu v členských státech a získala přístup k utajovaným informacím a prodala je. Společnost Anxun Information Technology Co. Ltd. navíc zaútočila na státní orgány různých třetích států a ohrozila cíle společné zahraniční a bezpečnostní politiky (SZBP) Unie stanovené v čl. 21 odst. 2 písm. a) až c) Smlouvy o Evropské unii. Společnost Anxun Information Technology získává z poskytovaných služeb významný hospodářský prospěch. Společnost Anxun Information Technology Co. Ltd. je tudíž odpovědná za kybernetické útoky s významným dopadem, které představují vnější hrozbu pro členské státy, jakož i za kybernetické útoky s významným dopadem na třetí státy.	16.3.2026“