2026/588

16.3.2026

DECYZJA RADY (WPZiB) 2026/588

z dnia 16 marca 2026 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) W ramach konsekwentnych, ukierunkowanych i skoordynowanych działań Unii przeciwko podmiotom stale powodującym zagrożenia w cyberprzestrzeni, w wykazie osób fizycznych i prawnych, podmiotów i organów podlegających środkom ograniczającym zawartym w załączniku do decyzji (UE) 2019/797 należy zamieścić dwie osoby fizyczne i trzy podmioty. Te osoby i podmioty są odpowiedzialne za cyberataki wywołujące poważne skutki i stanowiące zewnętrzne zagrożenie dla Unii lub jej państw członkowskich, lub są w nie zaangażowane.

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

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

W załączniku do decyzji (WPZiB) 2019/797 wprowadza się zmiany zgodnie z załącznikiem do niniejszej decyzji.

Artykuł 2

Niniejsza decyzja wchodzi w życie z dniem jej opublikowania w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono w Brukseli dnia 16 marca 2026 r.

W imieniu Rady

Przewodnicząca

K. KALLAS

([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: ELI: http://data.europa.eu/eli/dec/2019/797/oj).

ZAŁĄCZNIK

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

1) w sekcji „A. Osoby fizyczne” dodaje się wpisy w brzmieniu:

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
„18.	CHEN Cheng	陈诚 (pisownia chińska) Alias: Jesse Chen lengmo l3n6m0 Data urodzenia: 20.10.1984 Miejsce urodzenia: Yancheng, Jiangsu, Chiny Obywatelstwo: chińskie Płeć: mężczyzna	Chen Cheng jest chińskim biznesmenem, współzałożycielem i jednym z dyrektorów generalnych przedsiębiorstwa Anxun Information Technology Co Ltd. Jest również przedstawicielem prawnym oddziału tego przedsiębiorstwa w Syczuanie. Anxun Information Technology Co Ltd., znane również jako i-Soon, jest przedsiębiorstwem z siedzibą w Chińskiej Republice Ludowej, które oferuje usługi hakerskie do wynajęcia. Anxun Information Technology Co Ltd. prowadzi działania wymierzone w infrastrukturę krytyczną i krytyczne funkcje państwowe państw członkowskich, zdobywa dostęp do informacji niejawnych oraz sprzedaje te informacje. Anxun Information Technology Co Ltd. przeprowadza ponadto ataki na rządy różnych państw trzecich, stwarzając tym samym zagrożenie dla celów wspólnej polityki zagranicznej i bezpieczeństwa (WPZiB) Unii określonych w art. 21 ust. 2 lit. a)–c) Traktatu o Unii Europejskiej. Anxun Information Technology Co Ltd. czerpie istotne korzyści gospodarcze ze świadczonych usług. Anxun Information Technology Co Ltd. jest zatem odpowiedzialne za cyberataki wywołujące poważne skutki i stanowiące zewnętrzne zagrożenie dla Unii i jej państw członkowskich, a także za ataki przeciwko państwom trzecim. Z racji pełnionej funkcji Chen Cheng jest odpowiedzialny za cyberataki wywołujące poważne skutki i stanowiące zewnętrzne zagrożenie dla państw członkowskich, a także za cyberataki wywołujące poważne skutki dla państw trzecich, oraz jest zaangażowany w te cyberataki.	16.3.2026

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
19.	WU Haibo	吴海波 (pisownia chińska) Alias: shutdown shutd0wn Miejsce urodzenia: Chiny Obywatelstwo: chińskie Płeć: mężczyzna	Wu Haibo jest chińskim biznesmenem, współzałożycielem i jednym z dyrektorów generalnych przedsiębiorstwa Anxun Information Technology Co Ltd. Jest również przedstawicielem prawnym, prezesem i dyrektorem generalnym oddziału tego przedsiębiorstwa w Szanghaju (tzw. »bazy«). Pondato pełni obowiązki przedstawiciela prawnego oddziału tego przedsiębiorstwa w Syczuanie. Anxun Information Technology Co Ltd., znane również jako i-Soon, jest przedsiębiorstwem z siedzibą w Chińskiej Republice Ludowej, które oferuje usługi hakerskie do wynajęcia. Anxun Information Technology Co Ltd. prowadzi działania wymierzone w infrastrukturę krytyczną i krytyczne funkcje państwowe państw członkowskich, zdobywa dostęp do informacji niejawnych oraz sprzedaje te informacje. Anxun Information Technology Co Ltd. przeprowadza ponadto ataki na rządy różnych państw trzecich, stwarzając tym samym zagrożenie dla celów wspólnej polityki zagranicznej i bezpieczeństwa (WPZiB) Unii określonych w art. 21 ust. 2 lit. a)–c) Traktatu o Unii Europejskiej. Anxun Information Technology Co Ltd. czerpie istotne korzyści gospodarcze ze świadczonych usług. Anxun Information Technology Co Ltd. jest zatem odpowiedzialne za cyberataki wywołujące poważne skutki i stanowiące zewnętrzne zagrożenie dla państw członkowskich, a także za ataki przeciwko państwom trzecim. Wu Haibo był zaangażowany w kierowanie próbami cyberataków wywołujących poważne skutki dla państw członkowskich oraz w zachęcanie do takich prób. Z racji pełnionej funkcji jest odpowiedzialny za cyberataki wywołujące poważne skutki i stanowiące zewnętrzne zagrożenie dla państw członkowskich, a także za cyberataki wywołujące poważne skutki dla państw trzecich, oraz jest zaangażowany w te cyberataki.	16.3.2026”;

2) w sekcji „B. Osoby prawne, podmioty i organy” dodaje się wpisy w brzmieniu:

	Nazwa	Dane identyfikacyjne	Powody	Data umieszczenia
„5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (pisownia chińska) Alias: Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited Adres: Fenghao East Road, Room 103, Building 6, No. 9, Beijing Haidian District, China Miejsce rejestracji: Pekin, Chiny Data wpisu do rejestru: 2.9.2010 Ujednolicony numer zezwolenia na prowadzenie działalności: 91110108562135265P	Integrity Technology Group jest przedsiębiorstwem z siedzibą w Chińskiej Republice Ludowej, które zajmuje się cyberbezpieczeństwem i które ułatwiało cyberataki związane z zaawansowanym, trwałym zagrożeniem (APT) ze strony Flax Typhoon. Podmiot ten wykorzystywał produkty i technologie Integrity Technology Group do realizacji swoich działań związanych z eksploatacją sieci komputerowych. Produkty Integrity Technology Group są od tej pory wykorzystywane do naruszania bezpieczeństwa urządzeń podłączonych do internetu rzeczy i uzyskiwania do nich dostępu w państwach członkowskich, a także w krajach w całej Europie i na świecie. W latach 2022–2023 Flax Typhoon działający w cyberprzestrzeni uzyskał dostęp do co najmniej 65 600 urządzeń podłączonych do internetu rzeczy w sześciu państwach członkowskich, korzystając z produktów Integrity Technology Group. Produkty handlowe i infrastruktura handlowa Integrity Technology Group były zatem rutynowo wykorzystywane w cyberatakach wymierzonych w państwa członkowskie oraz państwa trzecie. W związku z tym, wpływając na systemy informatyczne związane z infrastrukturą cyfrową, Integrity Technology Group zapewnia wsparcie techniczne i materialne na potrzeby cyberataków wywołujących poważne skutki i stanowiących zewnętrzne zagrożenie dla państw członkowskich i państw trzecich.	16.3.2026

	Nazwa	Dane identyfikacyjne	Powody	Data umieszczenia
6.	Emennet Pasargad	Alias: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten Miejsce rejestracji: Teheran, Iran Numer w rejestrze: 554267 Główne miejsce prowadzenia działalności: Teheran, Iran	Emennet Pasargad jest irańskim podmiotem działającym w cyberprzestrzeni (przedsiębiorstwem), który atakuje wiele podmiotów, w szczególności w państwach członkowskich, a także w Stanach Zjednoczonych (USA). Działając pod nazwą »Anzu Team«, Emennet Pasargad zaatakował infrastrukturę cyfrową w Szwecji oraz naruszył bezpieczeństwo szwedzkiej usługi SMS, co dotknęło dużą liczbę osób. Ponadto podmiot ten, działając pod nazwą »Holy Souls«, naruszył bezpieczeństwo bazy danych abonentów francuskiego czasopisma satyrycznego »Charlie Hebdo« i oferował ją na sprzedaż w darknecie. Podczas igrzysk olimpijskich w Paryżu Emennet Pasargad naruszył bezpieczeństwo billboardów reklamowych i wyświetlał na nich kampanie dezinformacyjne. Próbował również ingerować w wybory prezydenckie w USA w 2020 r., zagrażając demokracji i praworządności poprzez uzyskanie poufnych informacji o wyborcach amerykańskich oraz uzyskanie nieuprawnionego dostępu do sieci komputerowej amerykańskiego przedsiębiorstwa medialnego. Emennet Pasargad jest zatem odpowiedzialny za cyberataki wywołujące poważne skutki i stanowiące zewnętrzne zagrożenie dla państw członkowskich oraz za cyberataki wywołujące poważne skutki dla państwa trzeciego.	16.3.2026

	Nazwa	Dane identyfikacyjne	Powody	Data umieszczenia
7.	Anxun Information Technology Co. Ltd	安洵信息技术有限公司 (pisownia chińska) Alias: i-Soon Adres: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai Ujednolicony numer zezwolenia na prowadzenie działalności: 91510105332025597A (oddział w Syczuanie) Ujednolicony numer zezwolenia na prowadzenie działalności: 91310116561906136G (oddział w Szanghaju) Strona internetowa: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win Nr telefonu: +862161119992, +8605645893417, +8613761671735, +864000665915 Adres e-mail: shutdown@163.com, isoon2015@126.com, tao_tingting@i-soon.net, li_ping@i-soon.net	Anxun Information Technology Co. Ltd jest przedsiębiorstwem z siedzibą w Chińskiej Republice Ludowej, które oferuje usługi hakerskie do wynajęcia. Prowadzi działania wymierzone w infrastrukturę krytyczną i krytyczne funkcje państwowe państw członkowskich, zdobywa dostęp do informacji niejawnych oraz sprzedaje te informacje. Anxun Information Technology Co. Ltd przeprowadza ponadto ataki na rządy różnych państw trzecich, stwarzając tym samym zagrożenie dla celów wspólnej polityki zagranicznej i bezpieczeństwa (WPZiB) Unii określonych w art. 21 ust. 2 lit. a)–c) Traktatu o Unii Europejskiej. Anxun Information Technology Co. Ltd czerpie istotne korzyści gospodarcze ze świadczonych usług. Anxun Information Technology Co. Ltd. jest zatem odpowiedzialne za cyberataki wywołujące poważne skutki i stanowiące zewnętrzne zagrożenie dla państw członkowskich, a także za cyberataki wywołujące poważne skutki dla państw trzecich.	16.3.2026”