



**ROZPORZĄDZENIE WYKONAWCZE RADY (UE) 2026/589**

**z dnia 16 marca 2026 r.**

**wykonujące rozporządzenie (UE) 2019/796 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim**

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Rady (UE) 2019/796 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim<sup>(1)</sup>, w szczególności jego art. 13 ust. 1,

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 rozporządzenie (UE) 2019/796.
- (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 I do rozporządzenia (UE) 2019/796 należy umieścić dwie osoby fizyczne i trzy podmioty. Te osoby fizyczne i podmioty są odpowiedzialne za cyberataki wywołujące poważne skutki i stanowiące zewnętrzne zagrożenie dla Unii lub jej państw członkowskich, lub są zaangażowane w takie cyberataki.
- (3) Należy zatem odpowiednio zmienić załącznik I do rozporządzenia (UE) 2019/796,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

*Artykuł 1*

W załączniku I do rozporządzenia (UE) 2019/796 wprowadza się zmiany zgodnie z załącznikiem do niniejszego rozporządzenia.

*Artykuł 2*

Niniejsze rozporządzenie wchodzi w życie z dniem jego opublikowania w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 16 marca 2026 r.

*W imieniu Rady*

*Przewodnicząca*

K. KALLAS

<sup>(1)</sup> Dz.U. L 129 I z 17.5.2019, s. 1, ELI: <http://data.europa.eu/eli/reg/2019/796/oj>.

W załączniku I do rozporządzenia (UE) 2019/796 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	<p>陈诚</p> <p>(pisownia chińska)</p> <p>Alias:</p> <p>Jesse Chen</p> <p>lengmo</p> <p>l3n6m0</p> <p>Data urodzenia: 20.10.1984</p> <p>Miejsce urodzenia: Yancheng, Jiangsu, Chiny</p> <p>Obywatelstwo: chińskie</p> <p>Płeć: męczyzna</p>	<p>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.</p> <p>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.</p> <p>Anxun Information Technology Co Ltd. czerpie istotne korzyści gospodarcze ze świadczonych usług.</p> <p>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.</p> <p>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.</p>	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	<p>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«). Ponadto pełni obowiązki przedstawiciela prawnego oddziału tego przedsiębiorstwa w Sycuanie.</p> <p>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 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.</p> <p>Anxun Information Technology Co Ltd. czerpie istotne korzyści gospodarcze ze świadczonych usług.</p> <p>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.</p> <p>Wu Haibo był zaangażowany w kierowanie próbami cyberataków wywołujących poważne skutki dla państw członkowskich oraz w zachęcanie do takich prób.</p> <p>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.</p>	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	<p>永信至诚科技集团股份有限公司 (pisownia chińska)</p> <p>Alias: Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited</p> <p>Adres: Fenghao East Road, Room 103, Building 6, No. 9, Beijing Haidian District, China</p> <p>Miejsce rejestracji: Pekin, Chiny</p> <p>Data wpisu do rejestru: 2.9.2010</p> <p>Ujednolicony numer zezwolenia na prowadzenie działalności: 91110108562135265P</p>	<p>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.</p> <p>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.</p>	16.3.2026

	Nazwa	Dane identyfikacyjne	Powody	Data umieszczenia
6.	Emennet Pasargad	<p>Alias: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten</p> <p>Miejsce rejestracji: Teheran, Iran</p> <p>Numer w rejestrze: 554267</p> <p>Główne miejsce prowadzenia działalności: Teheran, Iran</p>	<p>Emennet Pasargad jest irańskim podmiotem działającym w cyberprzestrzeni (przedsiębiorstwem), który atakuje wiele podmiotów, w szczególności w państwach członkowskich, a także w Stanach Zjednoczonych (USA).</p> <p>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 darkniecie. 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.</p> <p>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.</p>	16.3.2026

	Nazwa	Dane identyfikacyjne	Powody	Data umieszczenia
7.	Anxun Information Technology Co. Ltd	<p>安洵信息技术有限公司 (pisownia chińska)</p> <p>Alias: i-Soon</p> <p>Adres: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai</p> <p>Ujednolicony numer zezwolenia na prowadzenie działalności: 91510105332025597A (oddział w Syczuanie)</p> <p>Ujednolicony numer zezwolenia na prowadzenie działalności: 91310116561906136G (oddział w Szanghaju)</p> <p>Strona internetowa: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win</p> <p>Nr telefonu: +862161119992, +8605645893417, +8613761671735, +864000665915</p> <p>Adres e-mail: shutdown@163.com, isoon2015@126.com, tao_tingting@i-soon.net, li_ping@i-soon.net</p>	<p>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.</p> <p>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.</p>	16.3.2026”