

Bruselj, 10. marec 2026
(OR. en)

5134/26

LIMITE

CORLX 10
CFSP/PESC 17
CYBER 4
JAI 21
FIN 8

ZAKONODAJNI AKTI IN DRUGI INSTRUMENTI

Zadeva: SKLEP SVETA o spremembi Sklepa (SZVP) 2019/797 o omejevalnih ukrepih proti kibernetским napadom, ki ogrožajo Unijo ali njene države članice

SKLEP SVETA (SZVP) 2026/...

z dne ...

**o spremembi Sklepa (SZVP) 2019/797 o omejevalnih ukrepih
proti kibernetским napadom, ki ogrožajo Unijo ali njene države članice**

SVET EVROPSKE UNIJE –

ob upoštevanju Pogodbe o Evropski uniji in zlasti člena 29 Pogodbe,

ob upoštevanju predloga visokega predstavnika Unije za zunanje zadeve in varnostno politiko,

ob upoštevanju naslednjega:

- (1) Svet je 17. maja 2019 sprejel Sklep (SZVP) 2019/797¹.
- (2) Kot del stalnega, prilagojenega in usklajenega ukrepanja Unije proti vztrajnim akterjem na področju kibernetских groženj bi bilo treba na seznam fizičnih in pravnih oseb, subjektov in organov, za katere veljajo omejevalni ukrepi iz Priloge k Sklepu (SZVP) 2019/797, uvrstiti dve fizični osebi in tri subjekte. Ti osebi in subjekti so odgovorni za ali so vpleteni v kibernetiske napade s pomembnim učinkom, ki pomenijo zunanjo grožnjo Uniji ali njenim državam članicam.
- (3) Sklep (SZVP) 2019/797 bi bilo treba zato ustrezno spremeniti –

SPREJEL NASLEDNJI SKLEP:

¹ Sklep Sveta (SZVP) 2019/797 z dne 17. maja 2019 o omejevalnih ukrepih proti kibernetiskim napadom, ki ogrožajo Unijo ali njene države članice (UL L 129 I, 17.5.2019, str. 13, ELI: <http://data.europa.eu/eli/dec/2019/797/oj>).

Člen 1

Priloga k Sklepu (SZVP) 2019/797 se spremeni v skladu s Prilogo k temu sklepu.

Člen 2

Ta sklep začne veljati na dan objave v *Uradnem listu Evropske unije*.

V ..., ...

Za Svet

predsednik/predsednica

PRILOGA

Priloga k Sklepu (SZVP) 2019/797 se spremeni:

(1) pod naslovom „A. Fizične osebe“ se dodata naslednja vnosa:

	Ime in priimek	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
„18.	CHEN Cheng	陈诚 (kitajski zapis) Vzdevki: Jesse Chen lengmo l3n6m0 Datum rojstva: 20.10.1984 Kraj rojstva: Yancheng, Jiangsu, Kitajska Državljanstvo: kitajsko Spol: moški	Je kitajski poslovnež, soustanovitelj in eden od generalnih direktorjev podjetja Anxun Information Technology Co. Ltd. Je tudi pravni zastopnik sečuanske podružnice tega podjetja. Podjetje Anxun Information Technology Co. Ltd., znano tudi kot i-Soon, ima sedež v Ljudski republiki Kitajski (LRK) in ponuja v najem storitve hekanja. Cilj napadov podjetja Anxun Information Technology Co. Ltd. so bile kritična infrastruktura in najpomembnejše državne funkcije v državah članicah, pridobilo pa je dostop do tajnih podatkov in jih prodajalo. Poleg tega je podjetje Anxun Information Technology Co. Ltd. izvajalo napade na vlade različnih tretjih držav in s tem predstavljalo grožnjo ciljem skupne zunanje in varnostne politike (SZVP) Unije, kot so določeni v členu 21(2), točke (a) do (c), Pogodbe o Evropski uniji. Podjetje ima od zagotavljanja teh storitev precejšnjo gospodarsko korist.	+

+ UL: vstaviti datum začetka veljavnosti tega sklepa.

	Ime in priimek	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
			<p>Podjetje Anxun Information Technology Co. Ltd. je zato odgovorno za kibernetške napade s pomembnim učinkom, ki pomenijo zunanjo grožnjo Uniji in njenim državam članicam, in tudi za napade na tretje države.</p> <p>Na tej funkciji je odgovoren za kibernetške napade s pomembnim učinkom, ki pomenijo zunanjo grožnjo državam članicam, in za kibernetške napade s pomembnim učinkom, uperjene proti tretjim državam; poleg tega je v te napade tudi vpleten.</p>	

	Ime in priimek	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
19.	WU Haibo	<p>吴海波 (kitajski zapis) Vzdevki: shutdown shutd0wn Kraj rojstva: Kitajska Državljanstvo: kitajsko Spol: moški</p>	<p>Je kitajski poslovnež, soustanovitelj in eden od generalnih direktorjev podjetja Anxun Information Technology Co. Ltd. Je tudi pravni zastopnik, predsednik in generalni direktor šanghajske podružnice (glavne podružnice) tega podjetja. Poleg tega deluje kot pravni zastopnik sečuanske podružnice tega podjetja.</p> <p>Podjetje Anxun Information Technology Co. Ltd., znano tudi kot i-Soon, ima sedež v Ljudski republiki Kitajski (LRK) in ponuja v najem storitve hekanja. Cilj napadov Anxun Information Technology Co. Ltd. so bile kritična infrastruktura in najpomembnejše državne funkcije v državah članicah, pridobilo pa je dostop do tajnih podatkov in jih prodajalo. Poleg tega je podjetje Anxun Information Technology Co. Ltd. izvajalo napade na vlade različnih tretjih držav in s tem predstavljalo grožnjo ciljem skupne zunanje in varnostne politike (SZVP) Unije, kot so določeni v členu 21(2), točke (a) do (c), Pogodbe o Evropski uniji.</p> <p>Podjetje Anxun Information Technology Co. Ltd. ima od zagotavljanja teh storitev precejšnjo gospodarsko korist.</p>	+“;

+ UL: vstaviti datum začetka veljavnosti tega sklepa.

	Ime in priimek	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
			<p>Podjetje Anxun Information Technology Co. Ltd. je zato odgovorno za kibernetške napade s pomembnim učinkom, ki pomenijo zunanjo grožnjo državam članicam, in tudi za napade na tretje države.</p> <p>Wu Haibo je sodeloval pri vodenju in spodbujanju poskusov kibernetških napadov s pomembnim učinkom na države članice.</p> <p>Na tej funkciji je odgovoren za kibernetške napade s pomembnim učinkom, ki pomenijo zunanjo grožnjo državam članicam, in za kibernetške napade s pomembnim učinkom, uperjene proti tretjim državam; poleg tega je v te napade tudi vpleten.</p>	

(2) pod naslovom „B. Pravne osebe, subjekti in organi“ se dodajo naslednji vnosi:

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
„5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (kitajski zapis) tudi: Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited Naslov: Fenghao East Road, Room 103, Building 6, No. 9, Beijing Haidian District, China	Integrity Technology Group je podjetje za kibernetiko s sedežem v Ljudski republiki Kitajski (LRK), ki je omogočalo kibernetične napade, povezane s Advanced Persistent Threat (APT) Flax Typhoon. Skupina APT je proizvode in tehnologijo Integrity Technology Group uporabljala pri izvajanju svojih dejavnosti, povezanih z izrabljanjem računalniškega omrežja. Proizvodi Integrity Technology Group se od takrat uporabljajo za ogrožanje naprav in dostopa do interneta stvari v državah članicah ter v državah po Evropi in po svetu. Flax Typhoon je v letih 2022 in 2023 z uporabo proizvodov Integrity Technology Group imel dostop do najmanj 65 600 naprav interneta stvari v šestih državah članicah. Komerčni proizvodi in infrastruktura podjetja Integrity Technology Group so se zato rutinsko uporabljali v kibernetičnih napadih na države članice in tretje države. Integrity Technology Group zato z vplivanjem na informacijske sisteme, povezane z digitalno infrastrukturo, zagotavlja tehnično in materialno podporo za kibernetične napade s pomembnim učinkom, ki pomenijo zunanjo grožnjo državam članicam in tretjim državam.	+

+ UL: vstaviti datum začetka veljavnosti tega sklepa.

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
		Kraj vpisa: Peking, Kitajska Datum vpisa: 2.9.2010 Poenotena številka podjetja: 91110108562135265P		

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
6.	Emennet Pasargad	<p>tudi: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten</p> <p>Kraj vpisa: Teheran, Iran Številka vpisa: 554267</p> <p>Glavni kraj delovanja: Teheran, Iran</p>	<p>Je iranski kibernetški akter (podjetje), ki je si je za cilj napada izbral številne subjekte, zlasti v državah članicah in Združenih državah Amerike (ZDA).</p> <p>Pod vzdevkom „Anzu Team“ je izvedel napad na digitalno infrastrukturo na Švedskem in ogrozil švedsko storitev SMS, kar je prizadelo veliko število oseb. Poleg tega je pod vzdevkom „Holy Souls“ kompromitiral zbirko podatkov o naročnikih francoske satirične revije Charlie Hebdo in jo oglaševal za prodajo na temnem spletu. Med olimpijskimi igrami v Parizu je kompromitiral oglasne panoje in prikazoval dezinformacijske kampanje. Skušal se je vmešavati tudi v predsedniške volitve v ZDA leta 2020, s čimer je ogrožal demokracijo in pravno državo, saj je pridobil zaupne informacije o ameriških volivcih in nepooblaščen dostop do računalniškega omrežja enega od ameriških medijskih podjetij.</p> <p>Zato je odgovoren za kibernetške napade s pomembnim učinkom, ki pomenijo zunanjo grožnjo državam članicam, in za kibernetške napade s pomembnim učinkom, uperjene proti tretji državi.</p>	+

+ UL: vstaviti datum začetka veljavnosti tega sklepa.

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
7.	Anxun Information Technology Co. Ltd	<p>安洵信息技术有限公司 (kitajski zapis) tudi: i-Soon</p> <p>Naslov: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai</p> <p>Poenotena številka podjetja: 91510105332025597A (sečuanska podružnica)</p> <p>Poenotena številka podjetja: 91310116561906136G (šanghajska podružnica)</p>	<p>Podjetje Anxun Information Technology Co. Ltd. ima sedež v Ljudski republiki Kitajski (LRK) in ponuja v najem storitve hekanja. Njegov cilj je bila kritična infrastruktura in najpomembnejše državne funkcije v državah članicah, pridobilo pa je dostop do tajnih podatkov in jih prodajalo. Poleg tega je podjetje Anxun Information Technology Co. Ltd. izvajalo napade na vlade različnih tretjih držav in s tem predstavljalo grožnjo ciljem skupne zunanje in varnostne politike (SZVP) Unije, kot so določeni v členu 21(2), točke (a) do (c), Pogodbe o Evropski uniji. Podjetje Anxun Information Technology Co. Ltd. ima od zagotavljanja teh storitev precejšnjo gospodarsko korist.</p> <p>Zato je odgovorno za kibernetične napade s pomembnim učinkom, ki pomenijo zunanjo grožnjo državam članicam, in za kibernetične napade s pomembnim učinkom, uperjene proti tretjim državam.</p>	+“.

+ UL: vstaviti datum začetka veljavnosti tega sklepa.

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
		<p>Spletne strani: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win</p> <p>Telefonske številke: +862161119992, +8605645893417, +8613761671735, +864000665915</p> <p>E-naslovi: shutdown@163.com, isoon2015@126.com, tao_tingting@i-soon.net, li_ping@i-soon.net</p>		