2026/589

16.3.2026

RÅDETS GENNEMFØRELSESFORORDNING (EU) 2026/589

af 16. marts 2026

om gennemførelse af forordning (EU) 2019/796 om restriktive foranstaltninger til bekæmpelse af cyberangreb, der truer Unionen eller dens medlemsstater

RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Rådets forordning (EU) 2019/796 af 17. maj 2019 om restriktive foranstaltninger til bekæmpelse af cyberangreb, der truer Unionen eller dens medlemsstater [1], særlig artikel 13, stk. 1,

under henvisning til forslag fra Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik, og

ud fra følgende betragtninger:

(1) Den 17. maj 2019 vedtog Rådet forordning (EU) 2019/796.

(2) Som led i den fortsatte skræddersyede og koordinerede EU-indsats over for persistente cybertrusselsaktører bør to fysiske personer og tre enheder opføres på listen over fysiske og juridiske personer, enheder og organer, der er omfattet af restriktive foranstaltninger, i bilag I til forordning (EU) 2019/796. Disse fysiske personer og enheder er ansvarlige for eller er involveret i cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater.

(3) Bilag I til forordning (EU) 2019/796 bør derfor ændres i overensstemmelse hermed —

VEDTAGET DENNE FORORDNING:

Artikel 1

Bilag I til forordning (EU) 2019/796 ændres som angivet i bilaget til nærværende forordning.

Artikel 2

Denne forordning træder i kraft på dagen for offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 16. marts 2026.

På Rådets vegne

K. KALLAS

Formand

[1] EUT L 129 I af 17.5.2019, s. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj.

BILAG

I bilag I til forordning (EU) 2019/796 foretages følgende ændringer:

1) Følgende punkter tilføjes under overskriften »A. Fysiske personer«:

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
»18.	CHEN Cheng	陈诚 (kinesisk skrivemåde) Aliasser: Jesse Chen lengmo l3n6m0 Fødselsdato: 20.10.1984 Fødested: Yancheng, Jiangsu, Kina Nationalitet: kinesisk Køn: mand	Chen Cheng er en kinesisk forretningsmand, medstifter og en af direktørerne (driftsdirektør) for Anxun Information Technology Co. Ltd. Han er også juridisk repræsentant for denne virksomheds filial i Sichuan. Anxun Information Technology Co. Ltd., også kendt som i-Soon, er en virksomhed med hjemsted i Folkerepublikken Kina (Kina), der tilbyder »hacking for hire«-tjenester. Anxun Information Technology Co. Ltd. har haft kritisk infrastruktur og kritiske statslige funktioner i medlemsstaterne som mål og har tilgået og solgt klassificerede informationer. Desuden har Anxun Information Technology Co. Ltd. angrebet regeringer i forskellige tredjelande og udgør dermed en trussel mod målene for Unionens fælles udenrigs- og sikkerhedspolitik (FUSP), jf. artikel 21, stk. 2, litra a)-c), i traktaten om Den Europæiske Union. Anxun Information Technology Co. Ltd. drager en væsentlig økonomisk fordel af de leverede tjenester. Anxun Information Technology Co. Ltd. er derfor ansvarlig for cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod Unionen og dens medlemsstater, og for angreb mod tredjelande. Chen Cheng er i denne egenskab ansvarlig for og involveret i cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod medlemsstaterne, samt cyberangreb med betydelige konsekvenser for tredjelande.	16.3.2026

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
19.	WU Haibo	吴海波 (kinesisk skrivemåde) Aliasser: shutdown shutd0wn Fødested: Kina Nationalitet: kinesisk Køn: mand	Wu Haibo er en kinesisk forretningsmand, medstifter af og en af direktørerne (administrerende direktør) for Anxun Information Technology Co. Ltd. Han er også juridisk repræsentant, formand og direktør for filialen i Shanghai (»mothership«) i Anxun Information Technology Co. Ltd. Han fungerer desuden som juridisk repræsentant for dette selskabs filial i Sichuan. Anxun Information Technology Co. Ltd., også kendt som i-Soon, er en virksomhed med hjemsted i Folkerepublikken Kina (Kina), der tilbyder »hacking for hire«-tjenester. Anxun Information Technology Co. Ltd. har haft kritisk infrastruktur og kritiske statslige funktioner i medlemsstaterne som mål og har tilgået og solgt klassificerede informationer. Desuden har Anxun Information Technology Co. Ltd. angrebet regeringer i forskellige tredjelande, og udgør dermed en trussel mod målene for Unionens fælles udenrigs- og sikkerhedspolitik (FUSP), jf. artikel 21, stk. 2, litra a)-c), i traktaten om Den Europæiske Union. Anxun Information Technology Co. Ltd. drager en væsentlig økonomisk fordel af de leverede tjenester. Anxun Information Technology Co. Ltd. er derfor ansvarlig for cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod medlemsstaterne, og for angreb mod tredjelande. Wu Haibo var involveret i ledelsen af og tilskyndelsen til forsøg på cyberangreb med betydelige konsekvenser for medlemsstaterne. Han er i denne egenskab ansvarlig for og involveret i cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod medlemsstaterne, samt cyberangreb med betydelige konsekvenser for tredjelande.	16.3.2026«.

2) Følgende punkter tilføjes under overskriften »B. Juridiske personer, enheder og organer«:

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
»5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (kinesisk skrivemåde) Alias: Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited Adresse: Fenghao East Road, Room 103, Building 6, No. 9, Beijing Haidian District, China Registreringssted: Beijing, Kina Registreringsdato: 2.9.2010 Virksomhedsregistreringsnummer: 91110108562135265P	Integrity Technology Group er en cybersikkerhedsvirksomhed med hjemsted i Folkerepublikken Kina (Kina), der lettede cyberangreb i forbindelse med Advanced Persistent Threat (APT) Flax Typhoon. Denne APT anvendte Integrity Technology Groups produkter og teknologi til at udfolde sine aktiviteter til udnyttelse af computernetværk. Integrity Technology Groups produkter er siden da blevet anvendt til at kompromittere og få adgang til tingenes internet-enheder i medlemsstaterne, samt i lande i hele Europa og globalt. Mellem 2022 og 2023 tilgik Flax Typhoon mindst 65 600 tingenes internet-enheder i seks medlemsstater ved hjælp af Integrity Technology Groups produkter. Integrity Technology Groups kommercielle produkter og infrastruktur blev derfor rutinemæssigt anvendt i cyberangreb mod medlemsstaterne og tredjelande. Ved at påvirke informationssystemer vedrørende digital infrastruktur yder Integrity Technology Group som følge heraf teknisk og materiel støtte til cyberangreb med betydelige konsekvenser, som udgør en ekstern trussel mod medlemsstaterne og tredjelande.	16.3.2026

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
6.	Emennet Pasargad	Alias: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten Registreringssted: Teheran, Iran Registreringsnummer: 554267 Hovedforretningssted: Teheran, Iran	Emennet Pasargad er en iransk cyberaktør (virksomhed), der har målrettet angreb på en lang række enheder, navnlig i medlemsstaterne samt i De Forenede Stater (USA). Emennet Pasargad, der opererer under aliasset »Anzu Team«, rettede angreb mod digital infrastruktur i Sverige og kompromitterede en svensk SMS-tjeneste, hvilket berørte et stort antal personer. Ved at agere under navnet »Holy Souls« kompromitterede enheden endvidere abonnentdatabasen for det franske satiriske tidsskrift Charlie Hebdo og annoncerede, at det var til salg på det mørke net. Emennet Pasargad kompromitterede reklameskilte under De Olympiske Lege i Paris og førte desinformationskampagner. Emennet Pasargad forsøgte også at blande sig i det amerikanske præsidentvalg i 2020 og truede demokratiet og retsstatsprincippet ved at indhente fortrolige amerikanske vælgeroplysninger og opnå uautoriseret adgang til en amerikansk medievirksomheds computernetværk. Emennet Pasargad er derfor ansvarlig for cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod medlemsstaterne, og for cyberangreb med betydelige konsekvenser for et tredjeland.	16.3.2026

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
7.	Anxun Information Technology Co. Ltd.	安洵信息技术有限公司 (kinesisk skrivemåde) Alias: i-Soon Adresse: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai Virksomhedsregistreringsnummer: 91510105332025597A (filial i Sichuan) Virksomhedsregistreringsnummer: 91310116561906136G (filial i Shanghai) Websted: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win Telefonnumre: +862161119992, +8605645893417, +8613761671735, +864000665915 E-mail: shutdown@163.com, isoon2015@126.com, tao_tingting@i-soon.net, li_ping@i-soon.net	Anxun Information Technology Co. Ltd. er en virksomhed med hjemsted i Folkerepublikken Kina (Kina), der tilbyder »hacking for hire«-tjenester. Den har haft kritisk infrastruktur og kritiske statslige funktioner i medlemsstaterne som mål og har tilgået og solgt klassificerede informationer. Desuden har Anxun Information Technology Co. Ltd. angrebet regeringer i forskellige tredjelande, og udgør dermed en trussel mod mål for Unionens fælles udenrigs- og sikkerhedspolitik (FUSP), jf. artikel 21, stk. 2, litra a)-c), i traktaten om Den Europæiske Union. Anxun Information Technology Co. Ltd. drager en væsentlig økonomisk fordel af de leverede tjenester. Anxun Information Technology Co. Ltd. er derfor ansvarlig for cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod medlemsstaterne, samt cyberangreb med betydelige konsekvenser for tredjelande.	16.3.2026«

ELI: http://data.europa.eu/eli/reg_impl/2026/589/oj