2026/589

16.3.2026

RÅDETS GENOMFÖRANDEFÖRORDNING (EU) 2026/589

av den 16 mars 2026

om genomförande av förordning (EU) 2019/796 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater

EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av rådets förordning (EU) 2019/796 av den 17 maj 2019 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater [1], särskilt artikel 13.1,

med beaktande av förslaget från unionens höga representant för utrikes frågor och säkerhetspolitik, och

av följande skäl:

(1) Den 17 maj 2019 antog rådet förordning (EU) 2019/796.

(2) Som en del i de kontinuerliga, skräddarsydda och samordnade unionsinsatserna mot aktörer som utgör ett ihållande cyberhot bör två fysiska personer och tre enheter föras upp på förteckningen över fysiska och juridiska personer, enheter och organ som är föremål för restriktiva åtgärder som anges i bilaga I till förordning (EU) 2019/796. Dessa fysiska personer och enheter är ansvariga för eller inblandade i cyberattacker med en betydande effekt som utgör ett externt hot för unionen eller dess medlemsstater.

(3) Bilaga I till förordning (EU) 2019/796 bör därför ändras i enlighet med detta.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Bilaga I till förordning (EU) 2019/796 ska ändras i enlighet med bilagan till den här förordningen.

Artikel 2

Denna förordning träder i kraft samma dag som den offentliggörs i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 16 mars 2026.

På rådets vägnar

K. KALLAS

Ordförande

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

BILAGA

Bilaga I till förordning (EU) 2019/796 ska ändras på följande sätt:

1. Följande poster ska läggas till under rubriken ”A. Fysiska personer”:

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
”18.	CHEN Cheng	陈诚 (kinesisk skrift) Alias: Jesse Chen lengmo l3n6m0 Födelsedatum: 20.10.1984 Födelseort: Yancheng, Jiangsu, Kina Nationalitet: kinesisk Kön: man	Chen Cheng är en kinesisk affärsman som är medgrundare av och en av cheferna (operativ chef) vid Anxun Information Technology Co. Ltd. Han är också juridiskt ombud för företagets filial i Sichuan. Anxun Information Technology Co. Ltd., även känt som i-Soon, är ett företag baserat i Folkrepubliken Kina som erbjuder ’hackningstjänster på beställning’. Anxun Information Technology Co. Ltd. har angripit kritisk infrastruktur och kritiska statliga funktioner i medlemsstaterna och skaffat sig tillgång till och sålt säkerhetsskyddsklassificerade uppgifter. Anxun Information Technology Co. Ltd. har vidare angripit olika tredjeländers regeringar vilket utgör ett hot mot målen för unionens gemensamma utrikes- och säkerhetspolitik (Gusp) som fastställs i artikel 21.2 a–c i fördraget om Europeiska unionen. Anxun Information Technology Co. Ltd. erhåller stor ekonomisk fördel av de tillhandahållna tjänsterna. Anxun Information Technology Co. Ltd. är därmed ansvarigt för cyberattacker med en betydande effekt som utgör ett externt hot för unionen och dess medlemsstater samt attacker mot tredjeländer. I sin roll är Chen Cheng ansvarig för och inblandad i dels cyberattacker med en betydande effekt som utgör ett externt hot för medlemsstaterna, dels cyberattacker med en betydande effekt på tredjeländer.	16.3.2026

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
19.	WU Haibo	吴海波 (kinesisk skrift) Alias: shutdown shutd0wn Födelseort: Kina Nationalitet: kinesisk Kön: man	Wu Haibo är en kinesisk affärsman som är medgrundare av och en av cheferna (verkställande direktör) vid Anxun Information Technology Co. Ltd. Han är också juridiskt ombud, ordförande och chef för Anxun Information Technology Co. Ltds filial i Shanghai ('moderskeppet'). Dessutom agerar han som juridiskt ombud för det företagets filial i Sichuan. Anxun Information Technology Co. Ltd., alias i-Soon, är ett företag baserat i Folkrepubliken Kina som erbjuder 'hackningstjänster på beställning'. Anxun Information Technology Co. Ltd. har angripit kritisk infrastruktur och kritiska statliga funktioner i medlemsstaterna och skaffat sig tillgång till och sålt säkerhetsskyddsklassificerade uppgifter. Anxun Information Technology Co. Ltd. har vidare angripit olika tredjeländers regeringar vilket utgör ett hot mot målen för unionens gemensamma utrikes- och säkerhetspolitik (Gusp) som fastställs i artikel 21.2 a–c i fördraget om Europeiska unionen. Anxun Information Technology Co. Ltd. erhåller stor ekonomisk fördel av de tillhandahållna tjänsterna. Anxun Information Technology Co. Ltd. är därför ansvarigt för cyberattacker med en betydande effekt som utgör ett externt hot för medlemsstaterna samt attacker mot tredjeländer. Wu Haibo var inblandad i ledningen och uppmuntrandet av försök till cyberattacker med en betydande effekt mot medlemsstaterna. I sin roll är han ansvarig för och inblandad i dels cyberattacker med en betydande effekt som utgör ett externt hot för medlemsstaterna, dels cyberattacker med en betydande effekt på tredjeländer.	16.3.2026”

2. Följande poster ska läggas till under rubriken ”B. Juridiska personer, enheter och organ”:

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
”5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (kinesisk skrift) Alias: Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited Adress: Fenghao East Road, Room 103, Building 6, No. 9, Beijing Haidian District, China Registreringsort: Peking, Kina Registreringsdatum: 2.9.2010 Registreringsnummer (Unified Social Credit Code): 91110108562135265P	Integrity Technology Group är ett cybersäkerhetsföretag baserat i Folkrepubliken Kina som underlättat cyberattacker med koppling till Advanced Persistent Threat (APT) Flax Typhoon. Denna APT-grupp använde Integrity Technology Groups produkter och teknik för att utnyttja datornät. Integrity Technology Groups produkter har använts sedan dess för att äventyra och få tillgång till anordningar för sakernas internet i medlemsstater, samt länderna runt om i Europa och globalt. Mellan 2022 och 2023 skaffade Flax Typhoon sig tillgång till minst 65 600 anordningar för sakernas internet i sex medlemsstater med hjälp av Integrity Technology Groups produkter. Integrity Technology Groups kommersiella produkter och infrastruktur har således rutinmässigt använts i cyberattacker mot medlemsstater och tredjeländer. Genom att påverka informationssystem som rör digital infrastruktur tillhandahåller Integrity Technology Group därmed tekniskt och materiellt stöd till cyberattacker med en betydande effekt som utgör ett externt hot för medlemsstater och tredjeländer.	16.3.2026

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
6.	Emennet Pasargad	Alias: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten Registreringsort: Teheran, Iran Registreringsnummer: 554267 Huvudsakligt verksamhetsställe: Teheran, Iran	Emennet Pasargad är en iransk cyberaktör (företag) som har angripit ett flertal enheter, särskilt i medlemsstaterna samt i Förenta staterna (USA). Emennet Pasargad, som verkar under aliaset 'Anzu Team', har angripit digital infrastruktur i Sverige och komprometterat en svensk sms-tjänst, vilket påverkade ett stort antal personer. Genom att agera under aliaset 'Holy Souls' har enheten också komprometterat den franska satirtidningen Charlie Hebdos prenumerantdatabas och erbjudit den till försäljning på den mörka webben. Emennet Pasargad komprometterade reklamskyltar under de olympiska spelen i Paris och visade desinformationskampanjer. Emennet Pasargad försökte även påverka det amerikanska presidentvalet 2020 genom att inhämta konfidentiella uppgifter om amerikanska väljare och skaffa sig obehörig åtkomst till ett amerikanskt medieföretags datornät, vilket hotade demokratin och rättsstatens principer. Emennet Pasargad är därmed ansvarigt för cyberattacker med en betydande effekt som utgör ett externt hot för medlemsstaterna och för cyberattacker med en betydande effekt på ett tredjeland.	16.3.2026

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
7.	Anxun Information Technology Co. Ltd.	安洵信息技术有限公司 (kinesisk skrift) Alias: i-Soon Adress: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai Registreringsnummer (Unified Social Credit Code): 91510105332025597A (filialen i Sichuan) Registreringsnummer (Unified Social Credit Code): 91310116561906136G (filialen i Shanghai) Webbplats: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win Telefonnummer: +862161119992, +8605645893417, +8613761671735, +864000665915 E-post: shutdown@163.com, isoon2015@126.com, tao_tingting@i-soon.net, li_ping@i-soon.net	Anxun Information Technology Co. Ltd. är ett företag baserat i Folkrepubliken Kina som erbjuder 'hackningstjänster på beställning'. Företaget har angripit kritisk infrastruktur och kritiska statliga funktioner i medlemsstaterna och skaffat sig tillgång till och sålt säkerhetsskyddsklassificerade uppgifter. Anxun Information Technology Co. Ltd. har vidare angripit olika tredjeländers regeringar vilket utgör ett hot mot målen för unionens gemensamma utrikes- och säkerhetspolitik (Gusp) som fastställs i artikel 21.2 a–c i fördraget om Europeiska unionen. Anxun Information Technology Co. Ltd. erhåller stor ekonomisk fördel av de tillhandahållna tjänsterna. Anxun Information Technology Co. Ltd. är därmed ansvarigt för cyberattacker med en betydande effekt som utgör ett externt hot för medlemsstaterna, samt för cyberattacker med en betydande effekt på tredjeländer.	16.3.2026”

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