2026/588

16.3.2026

ΑΠΟΦΑΣΗ (ΚΕΠΠΑ) 2026/588 ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

της 16ης Μαρτίου 2026

για την τροποποίηση της απόφασης (ΚΕΠΠΑ) 2019/797 σχετικά με περιοριστικά μέτρα κατά κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της

ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

Έχοντας υπόψη τη Συνθήκη για την Ευρωπαϊκή Ένωση, και ιδίως το άρθρο 29,

Έχοντας υπόψη την πρόταση του Ύπατου Εκπροσώπου της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας,

Εκτιμώντας τα ακόλουθα:

(1) Στις 17 Μαΐου 2019 το Συμβούλιο εξέδωσε την απόφαση (ΚΕΠΠΑ) 2019/797 ([1]).

(2) Στο πλαίσιο της διαρκούς, εξατομικευμένης και συντονισμένης δράσης της Ένωσης κατά των επίμονων παραγόντων κυβερνοαπειλών, δύο φυσικά πρόσωπα και τρεις οντότητες θα πρέπει να περιληφθούν στον κατάλογο του παραρτήματος της απόφασης (ΚΕΠΠΑ) 2019/797, ο οποίος περιέχει φυσικά και νομικά πρόσωπα, οντότητες και φορείς που τελούν υπό περιοριστικά μέτρα. Τα πρόσωπα και οι οντότητες αυτές ευθύνονται για κυβερνοεπιθέσεις με σημαντικό αντίκτυπο που αποτελούν εξωτερική απειλή για την Ένωση ή τα κράτη μέλη της, ή εμπλέκονται σε τέτοιες κυβερνοεπιθέσεις.

(3) Η απόφαση (ΚΕΠΠΑ) 2019/797 θα πρέπει, συνεπώς, να τροποποιηθεί αναλόγως,

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΑΠΟΦΑΣΗ:

Άρθρο 1

Το παράρτημα της απόφασης (ΚΕΠΠΑ) 2019/797 τροποποιείται σύμφωνα με το παράρτημα της παρούσας απόφασης.

Άρθρο 2

Η παρούσα απόφαση αρχίζει να ισχύει την ημέρα δημοσίευσής της στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Βρυξέλλες, 16 Μαρτίου 2026.

Για το Συμβούλιο

Η Πρόεδρος

K. KALLAS

([1]) Απόφαση (ΚΕΠΠΑ) 2019/797 του Συμβουλίου, της 17ης Μαΐου 2019, σχετικά με περιοριστικά μέτρα κατά κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της (ΕΕ L 129 I της 17.5.2019, σ. 13, ELI: http://data.europa.eu/eli/dec/2019/797/oj).

ΠΑΡΑΡΤΗΜΑ

Το παράρτημα της απόφασης (ΚΕΠΠΑ) 2019/797 τροποποιείται ως εξής:

1. Οι ακόλουθες καταχωρίσεις προστίθενται κάτω από την επικεφαλίδα «Α. Φυσικά πρόσωπα»:

	Όνομα	Στοιχεία ταυτότητας	Λόγοι	Ημερομηνία καταχώρισης
«18.	CHEN Cheng	陈诚 (κινεζική γραφή) Άλλως: Jesse Chen lengmo l3n6m0 Ημερομηνία γέννησης: 20.10.1984 Τόπος γέννησης: Yancheng, Jiangsu, Κίνα Ιθαγένεια: κινεζική Φύλο: άρρεν	Ο Chen Cheng είναι Κινέζος επιχειρηματίας, συνιδρυτής και εκ των γενικών διευθυντών (Γενικός Διευθυντής Επιχειρήσεων) της εταιρείας Anxun Information Technology Co, Ltd. Είναι επίσης νόμιμος εκπρόσωπος του υποκαταστήματός της στο Sichuan της εν λόγω εταιρείας. Η Anxun Information Technology Co. Ltd, γνωστή και ως i-Soon, είναι εταιρεία που εδρεύει στη Λαϊκή Δημοκρατία της Κίνας και προσφέρει υπηρεσίες χάκινγκ επί πληρωμή. Έχει πλήξει κρίσιμες υποδομές και κρίσιμες κρατικές λειτουργίες κρατών μελών, έχει δε προσπελάσει και πωλήσει διαβαθμισμένες πληροφορίες. Επιπλέον, η Anxun Information Technology Co. Ltd έχει επιτεθεί σε κυβερνήσεις διαφόρων τρίτων χωρών, με αποτέλεσμα να θέτει σε απειλή τους στόχους της κοινής εξωτερικής πολιτικής και πολιτικής ασφαλείας (ΚΕΠΠΑ), της Ένωσης, όπως καθορίστηκαν στο άρθρο 21 παράγραφος (2), στοιχεία (α) έως (γ) της Συνθήκης της Ευρωπαϊκής Ένωσης. Η Anxun Information Technology Co Ltd αποκομίζει σημαντικό οικονομικό όφελος από τις παρεχόμενες υπηρεσίες. Συνεπώς, η Anxun Information Technology Co Ltd ευθύνεται για κυβερνοεπιθέσεις με σημαντικό αντίκτυπο που αποτελούν τόσο εξωτερική απειλή για την Ένωση και τα κράτη μέλη της όσο και επιθέσεις ενάντια σε τρίτες χώρες. . Λόγω της θέσης του, ο Chen Cheng ευθύνεται για κυβερνοεπιθέσεις με σημαντικό αντίκτυπο που αποτελούν εξωτερική απειλή για τα κράτη μέλη και για κυβερνοεπιθέσεις με σημαντικό αντίκτυπο κατά τρίτων κρατών, και εμπλέκεται σε τέτοιου είδους κυβερνοεπιθέσεις.	16.3.2026

	Όνομα	Στοιχεία ταυτότητας	Λόγοι	Ημερομηνία καταχώρισης
19.	WU Haibo	吴海波 (κινεζική γραφή) Άλλως: shutdown shutd0wn Τόπος γέννησης: Κίνα Ιθαγένεια: κινεζική Φύλο: άρρεν	Ο Wu Haibo είναι Κινέζος επιχειρηματίας, συνιδρυτής και εκ των γενικών διευθυντών (CEO Διευθύνων Σύμβουλος) της εταιρείας Anxun Information Technology Co Ltd. Είναι επίσης νόμιμος εκπρόσωπος, πρόεδρος και γενικός διευθυντής του υποκαταστήματος της Anxun Information Technology Co. Ltd στη Σαγκάη, το οποίο λειτουργεί σαν αρχηγείο της εταιρείας. Εκτελεί επίσης καθήκοντα νόμιμου εκπροσώπου του υποκαταστήματος της εν λόγω εταιρείας στο Sichuan. Η Anxun Information Technology Co Ltd, γνωστή και ως i-Soon, εδρεύει στη Λαϊκή Δημοκρατία της Κίνας (ΛΔΚ) και προσφέρει υπηρεσίες χάκινγκ επί πληρωμή. Η Anxun Information Technology Co Ltd έχει πλήξει κρίσιμες υποδομές και κρίσιμες κρατικές λειτουργίες κρατών μελών, έχει δε προσπελάσει και πωλήσει διαβαθμισμένες πληροφορίες. Επιπλέον, η Anxun Information Technology Co Ltd έχει επιτεθεί σε κυβερνήσεις διαφόρων τρίτων χωρών με αποτέλεσμα να θέτει σε απειλή τους στόχους της κοινής εξωτερικής πολιτικής και πολιτικής ασφαλείας (ΚΕΠΠΑ), όπως καθορίστηκαν στο άρθρο 21 παράγραφος (2), στοιχεία (α) έως (γ) της Συνθήκης της Ευρωπαϊκής Ένωσης. Η Anxun Information Technology Co Ltd αποκομίζει σημαντικό οικονομικό όφελος από τις παρεχόμενες υπηρεσίες. Συνεπώς, η Anxun Information Technology Co Ltd ευθύνεται για κυβερνοεπιθέσεις με σημαντικό αντίκτυπο που αποτελούν όχι μόνο εξωτερική απειλή για τα κράτη μέλη αλλά έχουν πλήξει και Τρίτες χώρες. Ο Wu Haibo, έχει εμπλοκή στην κατεύθυνση και ενθάρρυνση αποπειρών κυβερνοεπιθέσεων με σημαντικό αντίκτυπο κατά κρατών μελών. Λόγω της θέσης του, ευθύνεται για κυβερνοεπιθέσεις με σημαντικό αντίκτυπο που αποτελούν εξωτερική απειλή για τα κράτη μέλη και για κυβερνοεπιθέσεις με σημαντικό αντίκτυπο κατά τρίτων κρατών, και εμπλέκεται σε τέτοιου είδους κυβερνοεπιθέσεις.	16.3.2026»

2. Οι ακόλουθες καταχωρίσεις προστίθενται κάτω από την επικεφαλίδα «B. Νομικά πρόσωπα, οντότητες και φορείς»:

	Όνομα	Πληροφορίες ταυτοποίησης	Λόγοι	Ημερομηνία καταχώρισης
«5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (κινεζική γραφή) Άλλως: Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited Διεύθυνση: Fenghao East Road, Room 103, Building 6, No. 9, Beijing Haidian District, China Τόπος εγγραφής σε μητρώο: Πεκίνο, Κίνα Ημερομηνία εγγραφής σε μητρώο: 2.9.2010 Ενιαίος Κωδικός Κοινωνικής Πίστης: 91110108562135265P	Η Integrity Technology Group, επιχείρηση κυβερνοασφάλειας με έδρα στη Λαϊκή Δημοκρατία της Κίνας, έχει διευκολύνει κυβερνοεπιθέσεις συνδεόμενες με την Flax Typhoon, που συνιστά προηγμένη επίμονη απειλή (Advanced Persistent Threat – APT). Η εν λόγω ομάδα APT χρησιμοποίησε προϊόντα και τεχνολογία της Integrity Technology Group για να αναπτύξει δραστηριότητες εκμετάλλευσης υπολογιστικών δικτύων. Έκτοτε, προϊόντα της Integrity Technology Group έχουν χρησιμοποιηθεί για παρείσφρηση και πρόσβαση σε συσκευές του διαδικτύου των πραγμάτων σε κράτη μέλη, στην ευρύτερη Ευρώπη και παγκοσμίως. Μεταξύ 2022 και 2023, η Flax Typhoon απέκτησε πρόσβαση σε τουλάχιστον 65 600 συσκευές του διαδικτύου των πραγμάτων σε έξι κράτη μέλη χρησιμοποιώντας προϊόντα της Integrity Technology Group. Συνεπώς, εμπορικά προϊόντα και υποδομές της Integrity Technology Group χρησιμοποιήθηκαν συστηματικά σε κυβερνοεπιθέσεις κατά κρατών μελών και τρίτων χωρών. Ως εκ τούτου, προσβάλλοντας πληροφοριακά συστήματα σχετιζόμενα με ψηφιακές υποδομές, η Integrity Technology LTD παρέχει τεχνική και υλική υποστήριξη για κυβερνοεπιθέσεις με σημαντικό αντίκτυπο που την καθιστά εξωτερική απειλή για κράτη μέλη και τρίτες χώρες.	16.3.2026

	Όνομα	Πληροφορίες ταυτοποίησης	Λόγοι	Ημερομηνία καταχώρισης
6.	Emennet Pasargad	Άλλως: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten Τόπος εγγραφής σε μητρώο: Τεχεράνη, Ιράν Αριθμός μητρώου: 554267 Κύριος τόπος δραστηριοτήτων: Τεχεράνη, Ιράν	Η Emennet Pasargad (εταιρεία) είναι ιρανικός κυβερνοπαράγοντας που έχει πλήξει πολυάριθμες οντότητες, ιδίως στα κράτη μέλη, καθώς και στις Ηνωμένες Πολιτείες (ΗΠΑ). Η Emennet Pasargad, δραστηριοποιούμενη και ως “Anzu Team”, έπληξε ψηφιακές υποδομές στη Σουηδία και παρείσφρησε σε σουηδική υπηρεσία SMS, επηρεάζοντας μεγάλο αριθμό ατόμων. Επιπλέον, ενεργώντας και ως “Holy Souls”, η οντότητα παρείσφρησε στη βάση δεδομένων συνδρομητών του γαλλικού σατιρικού περιοδικού Charlie Hebdo και την έθεσε προς πώληση στο σκοτεινό διαδίκτυο. Η Emennet Pasargad παρείσφρησε σε διαφημιστικές πινακίδες κατά τη διάρκεια των Ολυμπιακών Αγώνων του Παρισιού και προέβαλε σε αυτές μηνύματα παραπληροφόρησης. Η Emennet Pasargad προσπάθησε επίσης να παρέμβει στις αμερικανικές προεδρικές εκλογές του 2020 αποκτώντας εμπιστευτικές πληροφορίες για Αμερικανούς ψηφοφόρους και παρεισφρέοντας σε υπολογιστικό δίκτυο αμερικανικής εταιρείας μέσων ενημέρωσης, απειλώντας έτσι τη δημοκρατία και το κράτος δικαίου. Συνεπώς, η Emennet Pasargad ευθύνεται για κυβερνοεπιθέσεις με σημαντικό αντίκτυπο που αποτελούν εξωτερική απειλή για τα κράτη μέλη, καθώς και για κυβερνοεπιθέσεις με σημαντικό αντίκτυπο κατά τρίτου κράτους.	16.3.2026

	Όνομα	Πληροφορίες ταυτοποίησης	Λόγοι	Ημερομηνία καταχώρισης
7.	Anxun Information Technology Co. Ltd	安洵信息技术有限公司 (κινεζική γραφή) Άλλως: I-Soon Διεύθυνση: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai Ενιαίος Κωδικός Κοινωνικής Πίστης: 91510105332025597A (υποκατάστημα Sichuan) Ενιαίος Κωδικός Κοινωνικής Πίστης: 91310116561906136G (υποκατάστημα Σαγκάης) Ιστότοπος: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win Τηλ: +862161119992, +8605645893417, +8613761671735, +864000665915 Email: shutdown@163.com, isoon2015@126.com, tao_tingting@i-soon.net, li_ping@i-soon.net	Η Anxun Information Technology Co, Ltd, είναι εταιρεία με έδρα στη Λαϊκή Δημοκρατία της Κίνας (ΛΔΚ), που προσφέρει υπηρεσίες χάκινγκ επί πληρωμή. Έχει πλήξει κρίσιμες υποδομές και κρίσιμες κρατικές λειτουργίες κρατών μελών, έχει δε προσπελάσει και πωλήσει διαβαθμισμένες πληροφορίες. Επιπλέον, η Anxun Information Technology Co Ltd έχει επιτεθεί σε κυβερνήσεις διαφόρων τρίτων χωρών, με αποτέλεσμα να θέτει σε απειλή του στόχους της κοινής εξωτερικής πολιτικής και πολιτικής ασφαλείας (ΚΕΠΠΑ) της Ένωσης, όπως καθορίστηκαν στο άρθρο 21 παράγραφος (2), στοιχεία (α) έως (γ) της Συνθήκης της Ευρωπαϊκής Ένωσης. Η Anxun Information Technology Co Ltd αποκομίζει σημαντικό οικονομικό όφελος από τις παρεχόμενες υπηρεσίες. Συνεπώς, η Anxun Information Technology Co Ltd ευθύνεται για κυβερνοεπιθέσεις με σημαντικό αντίκτυπο που αποτελούν εξωτερική απειλή για κράτη μέλη, καθώς και για κυβερνοεπιθέσεις με σημαντικό αντίκτυπο κατά τρίτων χωρών .	16.3.2026»

ELI: http://data.europa.eu/eli/dec/2026/588/oj