ΕΥΡΩΠΑΪΚΗ
ΕΠΙΤΡΟΠΗ

Στρασβούργο, 18.4.2023
COM(2023) 209 final

2023/0109 (COD)

Πρόταση

# ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

**σχετικά με τον καθορισμό μέτρων για την ενίσχυση της αλληλεγγύης και των ικανοτήτων της Ένωσης για την ανίχνευση, την προετοιμασία και την αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας**

# ΑΙΤΙΟΛΟΓΙΚΗ ΕΚΘΕΣΗ

## 1. ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΤΑΣΗΣ

- **Αιτιολόγηση και στόχοι της πρότασης**

Η παρούσα αιτιολογική έκθεση συνοδεύει την πρόταση πράξης για την αλληλεγγύη στον κυβερνοχώρο. Η χρήση των τεχνολογιών πληροφοριών και επικοινωνιών και η εξάρτηση από αυτές είναι πλέον θεμελιώδεις πτυχές σε όλους τους τομείς της οικονομικής δραστηριότητας, καθώς οι δημόσιες διοικήσεις, οι εταιρείες μας και οι πολίτες είναι πιο διασυνδεδεμένοι και αλληλεξαρτώμενοι από ποτέ, πέρα από τομείς και σύνορα. Αυτή η αύξηση της υιοθέτησης των ψηφιακών τεχνολογιών αυξάνει την έκθεση σε περιστατικά κυβερνοασφάλειας και τις πιθανές επιπτώσεις τους. Ταυτόχρονα, τα κράτη μέλη αντιμετωπίζουν αυξανόμενους κινδύνους κυβερνοασφάλειας και ένα συνολικά σύνθετο τοπίο απειλών, με σαφή κίνδυνο ταχείας πρόκλησης δευτερογενών επιπτώσεων από τα περιστατικά στον κυβερνοχώρο από ένα κράτος μέλος σε άλλα.

Επιπλέον, οι επιχειρήσεις στον κυβερνοχώρο ενσωματώνονται όλο και περισσότερο σε υβριδικές στρατηγικές και στρατηγικές πολέμου, με σημαντικές επιπτώσεις στον στόχο. Ειδικότερα, η στρατιωτική επίθεση της Ρωσίας κατά της Ουκρανίας συνοδεύεται από στρατηγική εχθρικών επιχειρήσεων στον κυβερνοχώρο, η οποία τέθηκε σε εφαρμογή πριν από την επίθεση και αλλάζει ριζικά την αντίληψη και την αξιολόγηση της συλλογικής ετοιμότητας της ΕΕ για τη διαχείριση κρίσεων κυβερνοασφάλειας και χρήζει επείγουσας αντιμετώπισης. Η απειλή πιθανού περιστατικού μεγάλης κλίμακας που θα προκαλέσει σημαντική διαταραχή και ζημία σε κρίσιμες υποδομές απαιτεί αυξημένη ετοιμότητα σε όλα τα επίπεδα του οικοσυστήματος κυβερνοασφάλειας της ΕΕ. Η απειλή αυτή υπερβαίνει τη στρατιωτική επίθεση της Ρωσίας κατά της Ουκρανίας και περιλαμβάνει συνεχείς κυβερνοαπειλές από κρατικούς και μη κρατικούς φορείς, οι οποίες είναι πιθανό να συνεχιστούν, δεδομένης της πληθώρας των συνασπιζόμενων με το κράτος εγκληματικών παραγόντων και παραγόντων χακτιβισμού (ακτιβιστών χάκερ) που εμπλέκονται στις τρέχουσες γεωπολιτικές εντάσεις. Τα τελευταία χρόνια, ο αριθμός των κυβερνοεπιθέσεων έχει αυξηθεί δραματικά, συμπεριλαμβανομένων των επιθέσεων στην αλυσίδα εφοδιασμού με στόχο την κυβερνοκατασκοπεία, την εγκατάσταση λυτρισμικού ή την πρόκληση διαταραχών. Το 2020 η επίθεση στην αλυσίδα εφοδιασμού της SolarWinds έπληξε περισσότερους από 18 000 οργανισμούς παγκοσμίως, συμπεριλαμβανομένων κυβερνητικών οργανισμών και μεγάλων εταιρειών. Τα σημαντικά περιστατικά κυβερνοασφάλειας μπορεί να προκαλούν δυσλειτουργίες πολύ σοβαρές για να αντιμετωπιστούν μεμονωμένα από ένα ή περισσότερα επηρεαζόμενα κράτη μέλη. Για τον λόγο αυτό, απαιτείται ενισχυμένη αλληλεγγύη σε επίπεδο Ένωσης για τον καλύτερο εντοπισμό, προετοιμασία και αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας.

Όσον αφορά τον εντοπισμό απειλών και περιστατικών στον κυβερνοχώρο, υπάρχει επείγουσα ανάγκη να αυξηθεί η ανταλλαγή πληροφοριών και να βελτιωθούν οι συλλογικές μας ικανότητες, προκειμένου να μειωθεί δραστικά ο χρόνος που απαιτείται για τον εντοπισμό

κυβερνοαπειλών, προτού αυτές προκαλέσουν μεγάλης κλίμακας ζημίες και κόστος[1]. Ενώ πολλές απειλές και περιστατικά κυβερνοασφάλειας έχουν δυνητικά διασυνοριακή διάσταση, λόγω της διασύνδεσης των ψηφιακών υποδομών, η ανταλλαγή σχετικών πληροφοριών μεταξύ των κρατών μελών παραμένει περιορισμένη. Η δημιουργία δικτύου διασυνοριακών κέντρων επιχειρήσεων ασφάλειας (SOC) για την ενίσχυση των ικανοτήτων εντοπισμού και αντίδρασης έχει ως στόχο να συμβάλει στην αντιμετώπιση αυτού του ζητήματος.

Όσον αφορά την ετοιμότητα και την αντιμετώπιση περιστατικών κυβερνοασφάλειας, επί του παρόντος υπάρχει περιορισμένη στήριξη σε επίπεδο Ένωσης και αλληλεγγύη μεταξύ των κρατών μελών. Στα συμπεράσματα που ενέκρινε τον Οκτώβριο του 2021, το Συμβούλιο τόνισε την ανάγκη να αντιμετωπιστούν αυτά τα κενά, καλώντας την Επιτροπή να υποβάλει πρόταση για ένα νέο ταμείο αντιμετώπισης καταστάσεων έκτακτης ανάγκης στον τομέα της κυβερνοασφάλειας[2].

Ο παρών κανονισμός εφαρμόζει επίσης τη στρατηγική κυβερνοασφάλειας της ΕΕ, η οποία εγκρίθηκε τον Δεκέμβριο του 2020[3] και στο πλαίσιο της οποίας εξαγγέλθηκε η δημιουργία μιας ευρωπαϊκής κυβερνοασπίδας για την ενίσχυση των ικανοτήτων εντοπισμού απειλών στον κυβερνοχώρο και ανταλλαγής πληροφοριών στην Ευρωπαϊκή Ένωση μέσω μιας ομοσπονδίας εθνικών και διασυνοριακών SOC.

Ο παρών κανονισμός βασίζεται στις πρώτες ενέργειες που έχουν ήδη αναπτυχθεί σε στενή συνεργασία με τα κύρια ενδιαφερόμενα μέρη και υποστηρίζονται από το πρόγραμμα «Ψηφιακή Ευρώπη» (DEP). Ειδικότερα, όσον αφορά τα SOC, στο πλαίσιο του προγράμματος εργασίας 2021-2022 για την κυβερνοασφάλεια του προγράμματος «Ψηφιακή ασφάλεια» πραγματοποιήθηκε πρόσκληση εκδήλωσης ενδιαφέροντος για την από κοινού προμήθεια εργαλείων και υποδομών για τη δημιουργία διασυνοριακών SOC, καθώς και πρόσκληση για επιχορηγήσεις ώστε να καταστεί δυνατή η ανάπτυξη ικανοτήτων των SOC που εξυπηρετούν δημόσιους και ιδιωτικούς οργανισμούς. Όσον αφορά την ετοιμότητα και την αντιμετώπιση περιστατικών, η Επιτροπή έχει καταρτίσει ένα βραχυπρόθεσμο πρόγραμμα για τη στήριξη των κρατών μελών, μέσω πρόσθετης χρηματοδότησης που διατίθεται στον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), με σκοπό την άμεση ενίσχυση της ετοιμότητας και των ικανοτήτων αντιμετώπισης σοβαρών περιστατικών στον κυβερνοχώρο. Και οι δύο δράσεις εκπονήθηκαν σε στενό συντονισμό με τα κράτη μέλη. Ο παρών κανονισμός αντιμετωπίζει τις ανεπάρκειες και ενσωματώνει πληροφορίες από τις εν λόγω δράσεις.

---

1 Σύμφωνα με έκθεση του Ponemon Institute και της IBM Security, ο μέσος χρόνος για τον εντοπισμό παραβίασης το 2022 ήταν 207 ημέρες, ενώ απαιτούνταν 70 επιπλέον ημέρες για την ανάσχεση της παραβίασης. Ταυτόχρονα, το 2022, οι παραβιάσεις δεδομένων με κύκλο ζωής άνω των 200 ημερών είχαν μέσο κόστος 4,86 εκατ. EUR, έναντι 3,74 εκατ. EUR όταν ο κύκλος ζωής δεν υπερέβαινε τις 200 ημέρες («Cost of a data breach 2022», https://www.ibm.com/reports/data-breach).

2 Συμπεράσματα του Συμβουλίου σχετικά με τη διαμόρφωση της στάσης της Ευρωπαϊκής Ένωσης στον κυβερνοχώρο, τα οποία εγκρίθηκαν από το Συμβούλιο κατά τη σύνοδό του στις 23 Μαΐου 2022 (9364/22).

3 Κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο «Η στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία» [JOIN(2020) 18 final].

Τέλος, η παρούσα πρόταση υλοποιεί τη δέσμευση, σύμφωνα με την κοινή ανακοίνωση για την κυβερνοάμυνα[4] που εκδόθηκε στις 10 Νοεμβρίου, για την εκπόνηση πρότασης για μια πρωτοβουλία αλληλεγγύης της ΕΕ για τον κυβερνοχώρο με τους ακόλουθους στόχους: ενίσχυση των κοινών ικανοτήτων ανίχνευσης, αντίληψης της κατάστασης και αντιμετώπισης στην ΕΕ, με σκοπό τη σταδιακή δημιουργία κυβερνοεφεδρείας σε επίπεδο ΕΕ με υπηρεσίες από αξιόπιστους ιδιωτικούς παρόχους και την υποστήριξη των δοκιμών κρίσιμων οντοτήτων.

Στο πλαίσιο αυτό, η Επιτροπή προτείνει την παρούσα πράξη για την αλληλεγγύη στον κυβερνοχώρο για την ενίσχυση της αλληλεγγύης σε επίπεδο Ένωσης με σκοπό την καλύτερη ανίχνευση, την προετοιμασία και την αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας μέσω των ακόλουθων ειδικών στόχων:

- ενίσχυση της κοινής ενωσιακής ανίχνευσης και αντίληψης της κατάστασης όσον αφορά τις απειλές και τα περιστατικά στον κυβερνοχώρο και, ως εκ τούτου, συμβολή στην ευρωπαϊκή τεχνολογική κυριαρχία στον τομέα της κυβερνοασφάλειας·
- αύξηση του βαθμού ετοιμότητας των κρίσιμων οντοτήτων σε ολόκληρη την ΕΕ και ενίσχυση της αλληλεγγύης με την ανάπτυξη κοινών ικανοτήτων αντιμετώπισης σημαντικών ή μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας, μεταξύ άλλων με την εξασφάλιση στήριξης για την αντιμετώπιση περιστατικών σε τρίτες χώρες, σε σύνδεση με το πρόγραμμα «Ψηφιακή Ευρώπη»·
- ενίσχυση της ανθεκτικότητας της Ένωσης και συμβολή στην αποτελεσματική αντίδραση με την εξέταση και την αξιολόγηση σημαντικών ή μεγάλης κλίμακας περιστατικών, συμπεριλαμβανομένης της άντλησης διδαγμάτων και, κατά περίπτωση, συστάσεων.

Οι στόχοι αυτοί υλοποιούνται μέσω των ακόλουθων δράσεων:

- ανάπτυξη πανευρωπαϊκής υποδομής SOC (ευρωπαϊκή κυβερνοασπίδα) για την οικοδόμηση και ενίσχυση κοινών ικανοτήτων ανίχνευσης και αντίληψης της κατάστασης.
- δημιουργία ενός μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο με σκοπό τη στήριξη των κρατών μελών όσον αφορά την προετοιμασία, την αντίδραση και την άμεση ανάκαμψη από σημαντικά και μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας. Η στήριξη για την αντιμετώπιση περιστατικών διατίθεται επίσης στα ευρωπαϊκά θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης (EUIBA).
- θέσπιση ενός ευρωπαϊκού μηχανισμού εξέτασης περιστατικών κυβερνοασφάλειας για την εξέταση και την αξιολόγηση συγκεκριμένων σημαντικών ή μεγάλης κλίμακας περιστατικών.

Η ευρωπαϊκή κυβερνοασπίδα και ο μηχανισμός έκτακτης ανάγκης στον κυβερνοχώρο θα στηριχθούν με χρηματοδότηση από το πρόγραμμα «Ψηφιακή Ευρώπη», το οποίο θα τροποποιηθεί με την παρούσα νομοθετική πράξη προκειμένου να καθοριστούν οι

[4] Κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο «Πολιτική της ΕΕ για την κυβερνοάμυνα» [JOIN(2022) 49 final].

προαναφερθείσες δράσεις, να παρασχεθεί χρηματοδοτική στήριξη για την ανάπτυξή τους και να αποσαφηνιστούν οι προϋποθέσεις για τη χορήγηση χρηματοδοτικής στήριξης.

**•Συνέπεια με τις ισχύουσες διατάξεις στον τομέα πολιτικής**

Το πλαίσιο της ΕΕ περιλαμβάνει διάφορες νομοθετικές πράξεις που έχουν ήδη θεσπιστεί ή προτείνονται σε επίπεδο Ένωσης για τη μείωση των τρωτών σημείων, την αύξηση της ανθεκτικότητας των κρίσιμων οντοτήτων έναντι κινδύνων κυβερνοασφάλειας και τη στήριξη της συντονισμένης διαχείρισης μεγάλης κλίμακας περιστατικών και κρίσεων στον τομέα της κυβερνοασφάλειας, ιδίως την οδηγία σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (NIS2)[5], την πράξη για την κυβερνοασφάλεια[6], την οδηγία για τις επιθέσεις κατά συστημάτων πληροφοριών[7] και τη σύσταση (ΕΕ) 2017/1584 της Επιτροπής για τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο[8].

Οι δράσεις που προτείνονται στο πλαίσιο της πράξης για την αλληλεγγύη στον κυβερνοχώρο καλύπτουν την αντίληψη της κατάστασης, την ανταλλαγή πληροφοριών, καθώς και τη στήριξη για την ετοιμότητα και την αντιμετώπιση περιστατικών στον κυβερνοχώρο. Οι δράσεις αυτές συνάδουν και στηρίζουν τους στόχους του ισχύοντος κανονιστικού πλαισίου σε επίπεδο Ένωσης, ιδίως βάσει της οδηγίας (ΕΕ) 2022/2555 (στο εξής: οδηγία NIS2). Η πράξη για την αλληλεγγύη στον κυβερνοχώρο θα αξιοποιήσει και θα στηρίξει ιδίως τα υφιστάμενα πλαίσια επιχειρησιακής συνεργασίας και διαχείρισης κρίσεων στον τομέα της κυβερνοασφάλειας, ιδίως το ευρωπαϊκό δίκτυο οργανισμών διασύνδεσης για κυβερνοκρίσεις (EU-CyCLONe) και το δίκτυο ομάδων αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (CSIRT).

Οι διασυνοριακές πλατφόρμες SOC θα πρέπει να αποτελέσουν μια νέα ικανότητα που θα συμπληρώνει το δίκτυο CSIRT, συγκεντρώνοντας και ανταλλάσσοντας δεδομένα σχετικά με απειλές κατά της κυβερνοασφάλειας από δημόσιες και ιδιωτικές οντότητες, ενισχύοντας την αξία των εν λόγω δεδομένων μέσω αναλύσεων εμπειρογνωμόνων και εργαλείων αιχμής και συμβάλλοντας στην ανάπτυξη των ικανοτήτων και της τεχνολογικής κυριαρχίας της Ένωσης.

---

5 Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2).

6 Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια).

7 Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Αυγούστου 2013, για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου.

8 Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία και με την τροποποίηση του κανονισμού (ΕΕ) 2019/1020 [COM(2022) 454 final].

Τέλος, η παρούσα πρόταση συνάδει με τη σύσταση του Συμβουλίου σχετικά με μια συντονισμένη προσέγγιση σε επίπεδο Ένωσης για την ενίσχυση της ανθεκτικότητας των κρίσιμων υποδομών[9], η οποία καλεί τα κράτη μέλη να λάβουν επείγοντα και αποτελεσματικά μέτρα και να συνεργαστούν καλόπιστα, αποδοτικά, με αλληλεγγύη και με συντονισμένο τρόπο μεταξύ τους, με την Επιτροπή και άλλες σχετικές δημόσιες αρχές, καθώς και με τις οικείες οντότητες, για την ενίσχυση της ανθεκτικότητας των κρίσιμων υποδομών που χρησιμοποιούνται για την παροχή βασικών υπηρεσιών στην εσωτερική αγορά.

- **Συνέπεια με άλλες πολιτικές της Ένωσης**

Η πρόταση συνάδει με άλλους μηχανισμούς και πρωτόκολλα έκτακτης ανάγκης για την αντιμετώπιση κρίσεων, όπως ο─μηχανισμός ολοκληρωμένης αντιμετώπισης πολιτικών κρίσεων (IPCR). Η πράξη για την αλληλεγγύη στον κυβερνοχώρο θα συμπληρώσει τα εν λόγω πλαίσια και πρωτόκολλα διαχείρισης κρίσεων παρέχοντας ειδική στήριξη για την ετοιμότητα και την αντιμετώπιση περιστατικών κυβερνοασφάλειας. Η πρόταση θα συνάδει επίσης με την εξωτερική δράση της ΕΕ για την αντιμετώπιση περιστατικών μεγάλης κλίμακας στο πλαίσιο της κοινής εξωτερικής πολιτικής και πολιτικής ασφαλείας (ΚΕΠΠΑ), μεταξύ άλλων μέσω της εργαλειοθήκης της ΕΕ για τη διπλωματία στον κυβερνοχώρο. Η πρόταση θα συμπληρώσει δράσεις που υλοποιούνται στο πλαίσιο του άρθρου 42 παράγραφος 7 της Συνθήκης για την Ευρωπαϊκή Ένωση ή σε καταστάσεις που ορίζονται στο άρθρο 222 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης.

Συμπληρώνει επίσης τον μηχανισμό πολιτικής προστασίας της Ένωσης (ΜΠΠΕ)[10] που θεσπίστηκε τον Δεκέμβριο του 2013 και συμπληρώθηκε με νέα νομοθετική πράξη που εκδόθηκε τον Μάιο του 2021[11], η οποία ενισχύει τους πυλώνες πρόληψης, ετοιμότητας και αντίδρασης του ΜΠΠΕ και παρέχει στην ΕΕ πρόσθετες ικανότητες για την αντιμετώπιση νέων κινδύνων στην Ευρώπη και στον κόσμο και ενισχύει το απόθεμα rescEU.

## 2. ΝΟΜΙΚΗ ΒΑΣΗ, ΕΠΙΚΟΥΡΙΚΟΤΗΤΑ ΚΑΙ ΑΝΑΛΟΓΙΚΟΤΗΤΑ

- **Νομική βάση**

Η νομική βάση της παρούσας πρότασης είναι το άρθρο 173 παράγραφος 3 και το άρθρο 322 παράγραφος 1 στοιχείο α) της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ). Το άρθρο 173 ΣΛΕΕ προβλέπει ότι η Ένωση και τα κράτη μέλη μεριμνούν ώστε να

[9] Σύσταση του Συμβουλίου, της 8ης Δεκεμβρίου 2022, σχετικά με συντονισμένη προσέγγιση σε επίπεδο Ένωσης με σκοπό την ενίσχυση της ανθεκτικότητας των κρίσιμων υποδομών (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ) (2023/C 20/01).

[10] Απόφαση αριθ. 1313/2013/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Δεκεμβρίου 2013, περί μηχανισμού πολιτικής προστασίας της Ένωσης (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).

[11] Κανονισμός (ΕΕ) 2021/836 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Μαΐου 2021, για την τροποποίηση της απόφασης αριθ. 1313/2013/ΕΕ περί μηχανισμού πολιτικής προστασίας της Ένωσης (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).

εξασφαλίζονται οι αναγκαίες προϋποθέσεις για την εξασφάλιση της ανταγωνιστικότητας της βιομηχανίας της Ένωσης. Ο παρών κανονισμός αποσκοπεί στην ενίσχυση της ανταγωνιστικής θέσης των τομέων της βιομηχανίας και των υπηρεσιών στην Ευρώπη σε ολόκληρη την ψηφιοποιημένη οικονομία και στη στήριξη του ψηφιακού μετασχηματισμού τους, διά της ενίσχυσης του επιπέδου κυβερνοασφάλειας στην ψηφιακή ενιαία αγορά. Ειδικότερα, αποσκοπεί στην αύξηση της ανθεκτικότητας των πολιτών, των επιχειρήσεων και των οντοτήτων που δραστηριοποιούνται σε τομείς κρίσιμης και εξαιρετικά κρίσιμης σημασίας έναντι των αυξανόμενων απειλών κατά της κυβερνοασφάλειας, οι οποίες μπορεί να έχουν καταστροφικές κοινωνικές και οικονομικές επιπτώσεις.

Η πρόταση βασίζεται στο άρθρο 322 παράγραφος 1 ΣΛΕΕ διότι περιλαμβάνει ειδικούς κανόνες μεταφοράς που παρεκκλίνουν από την αρχή της ετήσιας διάρκειας που προβλέπεται στον κανονισμό (ΕΕ, Ευρατόμ) 2018/1046 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (στο εξής: δημοσιονομικός κανονισμός)[12]. Για τους σκοπούς της χρηστής δημοσιονομικής διαχείρισης και λαμβανομένου υπόψη του απρόβλεπτου, έκτακτου και ειδικού χαρακτήρα του τοπίου της κυβερνοασφάλειας και των κυβερνοαπειλών, ο μηχανισμός έκτακτης ανάγκης για την κυβερνοασφάλεια θα πρέπει να επωφελείται από ορισμένο βαθμό ευελιξίας σε σχέση με τη δημοσιονομική διαχείριση, ιδίως δε διά της δυνατότητας αυτόματης μεταφοράς αχρησιμοποίητων πιστώσεων ανάληψης υποχρεώσεων και πιστώσεων πληρωμών για δράσεις που επιδιώκουν τους στόχους που ορίζονται στον κανονισμό στο επόμενο οικονομικό έτος. Δεδομένου ότι ο νέος αυτός κανόνας εγείρει ζητήματα σε σχέση με τον δημοσιονομικό κανονισμό, το ζήτημα αυτό μπορεί να εξεταστεί στο πλαίσιο των τρεχουσών διαπραγματεύσεων για την αναδιατύπωση του δημοσιονομικού κανονισμού.

- **Επικουρικότητα (σε περίπτωση μη αποκλειστικής αρμοδιότητας)**

Ο ισχυρός διασυνοριακός χαρακτήρας των απειλών κυβερνοασφάλειας, καθώς και ο αυξανόμενος αριθμός των κινδύνων και των περιστατικών, τα οποία έχουν δευτερογενείς επιπτώσεις σε διασυνοριακό επίπεδο, καθώς και σε τομείς και προϊόντα, συνεπάγονται ότι οι στόχοι της παρούσας παρέμβασης δεν μπορούν να επιτευχθούν αποτελεσματικά μόνο από τα κράτη μέλη και ότι απαιτείται κοινή δράση και αλληλεγγύη σε επίπεδο Ένωσης.

Η εμπειρία από την αντιμετώπιση των κυβερνοαπειλών που απορρέουν από τον πόλεμο κατά της Ουκρανίας, σε συνδυασμό με τα διδάγματα που αντλήθηκαν από μια άσκηση κυβερνοασφάλειας που διεξήχθη υπό τη γαλλική Προεδρία (EU CyCLES), έδειξε ότι θα πρέπει να αναπτυχθούν συγκεκριμένοι μηχανισμοί αμοιβαίας στήριξης, ιδίως η συνεργασία με τον ιδιωτικό τομέα, για την επίτευξη αλληλεγγύης σε επίπεδο ΕΕ. Στο πλαίσιο αυτό, στα συμπεράσματα της 23ης Μαΐου 2022 σχετικά με τη διαμόρφωση της στάσης της Ευρωπαϊκής Ένωσης στον κυβερνοχώρο, το Συμβούλιο καλεί την Επιτροπή να υποβάλει πρόταση για ένα

[12] Κανονισμός (ΕΕ, Ευρατόμ) 2018/1046 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Ιουλίου 2018, σχετικά με τους δημοσιονομικούς κανόνες που εφαρμόζονται στον γενικό προϋπολογισμό της Ένωσης (ΕΕ L 193 της 30.7.2018, σ. 1).

νέο ταμείο αντιμετώπισης καταστάσεων έκτακτης ανάγκης στον τομέα της κυβερνοασφάλειας.

Η στήριξη και οι δράσεις σε επίπεδο Ένωσης για την καλύτερη ανίχνευση των απειλών κυβερνοασφάλειας και την αύξηση των ικανοτήτων ετοιμότητας και αντίδρασης παρέχουν προστιθέμενη αξία, διότι αποφεύγεται η αλληλεπικάλυψη προσπαθειών σε ολόκληρη την Ένωση και τα κράτη μέλη. Θα οδηγήσουν σε καλύτερη αξιοποίηση των υφιστάμενων πάγιων στοιχείων και σε μεγαλύτερο συντονισμό και ανταλλαγή πληροφοριών σχετικά με τα διδάγματα που αντλούνται. Ο μηχανισμός έκτακτης ανάγκης στον κυβερνοχώρο προβλέπει επίσης την παροχή στήριξης σε τρίτες χώρες συνδεδεμένες με το πρόγραμμα «Ψηφιακή Ευρώπη» από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας.

Η στήριξη που παρέχεται μέσω των διαφόρων πρωτοβουλιών που θα θεσπιστούν και θα χρηματοδοτηθούν σε επίπεδο Ένωσης θα συμπληρώσει και δεν θα επικαλύπτει τις εθνικές ικανότητες όσον αφορά την ανίχνευση, την αντίληψη της κατάστασης, την ετοιμότητα και την αντίδραση σε κυβερνοαπειλές και περιστατικά.

**• Αναλογικότητα**

Οι δράσεις δεν υπερβαίνουν τα αναγκαία όρια για την επίτευξη των γενικών και ειδικών στόχων του κανονισμού. Οι δράσεις που προβλέπονται στον παρόντα κανονισμό δεν επηρεάζουν τις αρμοδιότητες των κρατών μελών όσον αφορά την εθνική ασφάλεια, τη δημόσια ασφάλεια, την πρόληψη, τη διερεύνηση, την ανίχνευση και τη δίωξη ποινικών αδικημάτων. Ούτε επηρεάζουν τις νομικές υποχρεώσεις των οντοτήτων που δραστηριοποιούνται σε τομείς κρίσιμης και εξαιρετικά κρίσιμης σημασίας να θεσπίζουν μέτρα κυβερνοασφάλειας, σύμφωνα με την οδηγία NIS 2.

Οι δράσεις που καλύπτονται από τον παρόντα κανονισμό είναι συμπληρωματικές των εν λόγω προσπαθειών και μέτρων, καθώς υποστηρίζουν τη δημιουργία υποδομών για την καλύτερη ανίχνευση και ανάλυση απειλών και παρέχουν στήριξη για δράσεις ετοιμότητας και αντίδρασης σε περίπτωση σημαντικών ή μεγάλης κλίμακας περιστατικών.

**• Επιλογή της νομικής πράξης**

Η πρόταση έχει τη μορφή κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου. Πρόκειται για το καταλληλότερο νομικό μέσο, δεδομένου ότι μόνο ένας κανονισμός, με τις άμεσα εφαρμοστέες νομικές διατάξεις του, μπορεί να παράσχει τον αναγκαίο βαθμό ομοιομορφίας που απαιτείται για τη δημιουργία και τη λειτουργία μιας ευρωπαϊκής κυβερνοασπίδας και ενός ευρωπαϊκού μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο, διά της πρόβλεψης παροχής στήριξης από το πρόγραμμα «Ψηφιακή Ευρώπη» για τη δημιουργία τους, καθώς και σαφών προϋποθέσεων για τη χρήση και τη διάθεση της εν λόγω στήριξης.

## 3. ΑΠΟΤΕΛΕΣΜΑΤΑ ΤΩΝ ΕΚ ΤΩΝ ΥΣΤΕΡΩΝ ΑΞΙΟΛΟΓΗΣΕΩΝ, ΤΩΝ ΔΙΑΒΟΥΛΕΥΣΕΩΝ ΜΕ ΤΑ ΕΝΔΙΑΦΕΡΟΜΕΝΑ ΜΕΡΗ ΚΑΙ ΤΩΝ ΕΚΤΙΜΗΣΕΩΝ ΕΠΙΠΤΩΣΕΩΝ

- **Διαβουλεύσεις με τα ενδιαφερόμενα μέρη**

Οι δράσεις του παρόντος κανονισμού θα υποστηρίζονται από το πρόγραμμα «Ψηφιακή Ευρώπη», το οποίο αποτέλεσε αντικείμενο ευρείας διαβούλευσης. Επιπλέον, θα βασιστούν στις πρώτες ενέργειες που έχουν προετοιμαστεί σε στενή συνεργασία με τα κύρια ενδιαφερόμενα μέρη. Όσον αφορά τα SOC, η Επιτροπή εκπόνησε έγγραφο προβληματισμού σχετικά με την ανάπτυξη διασυνοριακών πλατφορμών SOC και πρόσκληση εκδήλωσης ενδιαφέροντος σε στενή συνεργασία με τα κράτη μέλη στο πλαίσιο του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας (ECCC). Ως μέρος των εργασιών αυτών, διενεργήθηκε έρευνα σχετικά με τις εθνικές ικανότητες SOC και εξετάστηκαν κοινές προσεγγίσεις και τεχνικές απαιτήσεις στο πλαίσιο της τεχνικής ομάδας εργασίας του ECCC η οποία απαρτίζεται από εκπροσώπους των κρατών μελών. Επιπλέον, πραγματοποιήθηκαν ανταλλαγές με τη βιομηχανία, ιδίως μέσω της ομάδας εμπειρογνωμόνων για τα SOC που δημιουργήθηκε από τον ENISA και τον Ευρωπαϊκό οργανισμό για την ασφάλεια στον κυβερνοχώρο (ECSO).

Δεύτερον, όσον αφορά την ετοιμότητα και την αντιμετώπιση περιστατικών, η Επιτροπή έχει καταρτίσει ένα βραχυπρόθεσμο πρόγραμμα για τη στήριξη των κρατών μελών, μέσω πρόσθετης χρηματοδότησης που διατίθεται στον ENISA από το πρόγραμμα «Ψηφιακή Ευρώπη», με σκοπό την άμεση ενίσχυση της ετοιμότητας και των ικανοτήτων αντιμετώπισης σοβαρών περιστατικών στον κυβερνοχώρο. Οι παρατηρήσεις των κρατών μελών και της βιομηχανίας που συγκεντρώθηκαν κατά την υλοποίηση του εν λόγω βραχυπρόθεσμου προγράμματος παρέχουν ήδη πολύτιμες πληροφορίες που έχουν αξιοποιηθεί στο πλαίσιο της προετοιμασίας του προτεινόμενου κανονισμού για την αντιμετώπιση των ανεπαρκειών που εντοπίστηκαν. Πρόκειται για μια πρώτη ενέργεια σύμφωνα με τα συμπεράσματα του Συμβουλίου σχετικά με τη στάση στον κυβερνοχώρο, με τα οποία ζητείται από την Επιτροπή να υποβάλει πρόταση για ένα νέο ταμείο αντιμετώπισης καταστάσεων έκτακτης ανάγκης στον τομέα της κυβερνοασφάλειας.

Επιπλέον, στις 16 Φεβρουαρίου 2023 πραγματοποιήθηκε εργαστήριο με εμπειρογνώμονες των κρατών μελών σχετικά με τον μηχανισμό έκτακτης ανάγκης στον κυβερνοχώρο, βάσει εγγράφου προβληματισμού. Στο εν λόγω εργαστήριο συμμετείχαν όλα τα κράτη μέλη σε αυτό το εργαστήριο, ενώ έντεκα κράτη μέλη υπέβαλαν περαιτέρω γραπτές παρατηρήσεις.

- **Εκτίμηση επιπτώσεων**

Λόγω του επείγοντος χαρακτήρα της πρότασης, δεν διενεργήθηκε εκτίμηση επιπτώσεων. Οι δράσεις του παρόντος κανονισμού θα στηριχθούν από το πρόγραμμα «Ψηφιακή Ευρώπη» και συνάδουν με εκείνες που ορίζονται στον κανονισμό για το πρόγραμμα «Ψηφιακή Ευρώπη», ο οποίος αποτέλεσε αντικείμενο ειδικής εκτίμησης επιπτώσεων. Ο παρών κανονισμός δεν θα έχει σημαντικές διοικητικές ή περιβαλλοντικές επιπτώσεις πέραν εκείνων που έχουν ήδη

αξιολογηθεί στην εκτίμηση επιπτώσεων του κανονισμού για το πρόγραμμα «Ψηφιακή Ευρώπη».

Επιπλέον, αξιοποιεί τις πρώτες δράσεις που αναπτύχθηκαν σε στενή συνεργασία με τα κύρια ενδιαφερόμενα μέρη, όπως αναφέρεται ανωτέρω, και αποτελούν συνέχεια στην πρόσκληση των κρατών μελών προς την Επιτροπή να υποβάλει πρόταση για ένα νέο ταμείο αντιμετώπισης καταστάσεων έκτακτης ανάγκης στον τομέα της κυβερνοασφάλειας έως το τέλος του τρίτου τριμήνου του 2022.

Ειδικότερα, όσον αφορά την αντίληψη της κατάστασης και την ανίχνευση στο πλαίσιο της ευρωπαϊκής κυβερνοασπίδας, πραγματοποιήθηκε, στο πλαίσιο του προγράμματος εργασίας για την κυβερνοασφάλεια της περιόδου 2021-2022 βάσει του προγράμματος «Ψηφιακή Ευρώπη», πρόσκληση εκδήλωσης ενδιαφέροντος για την από κοινού προμήθεια εργαλείων και υποδομών για τη δημιουργία διασυνοριακών SOC, καθώς και πρόσκληση για επιχορηγήσεις ώστε να καταστεί δυνατή η ανάπτυξη ικανοτήτων των SOC που εξυπηρετούν δημόσιους και ιδιωτικούς οργανισμούς.

Στον τομέα της ετοιμότητας και της αντιμετώπισης περιστατικών, όπως προαναφέρθηκε, η Επιτροπή έχει καταρτίσει βραχυπρόθεσμο πρόγραμμα για τη στήριξη των κρατών μελών από το πρόγραμμα «Ψηφιακή Ευρώπη», το οποίο υλοποιείται από τον ENISA. Οι καλυπτόμενες υπηρεσίες περιλαμβάνουν δράσεις ετοιμότητας, όπως δοκιμές διείσδυσης κρίσιμων οντοτήτων για τον εντοπισμό τρωτών σημείων. Επίσης, ενισχύει τις δυνατότητες παροχής βοήθειας στα κράτη μέλη σε περίπτωση σοβαρού περιστατικού που επηρεάζει κρίσιμες οντότητες. Η εφαρμογή αυτού του βραχυπρόθεσμου προγράμματος από τον ENISA είναι σε εξέλιξη και έχουν ήδη παρασχεθεί σχετικές πληροφορίες που έχουν ληφθεί υπόψη κατά την προετοιμασία του παρόντος κανονισμού.

- **Θεμελιώδη δικαιώματα**

Συμβάλλοντας στην ασφάλεια των ψηφιακών πληροφοριών, η παρούσα πρόταση θα συμβάλει στην προστασία του δικαιώματος στην ελευθερία και την ασφάλεια σύμφωνα με το άρθρο 6 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ, καθώς και του δικαιώματος στον σεβασμό της ιδιωτικής και οικογενειακής ζωής σύμφωνα με το άρθρο 7 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ. Διά της προστασίας των επιχειρήσεων από οικονομικά επιζήμιες κυβερνοεπιθέσεις, η πρόταση θα συμβάλει επίσης στην επιχειρηματική ελευθερία σύμφωνα με το άρθρο 16 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ, καθώς και στο δικαίωμα ιδιοκτησίας σύμφωνα με το άρθρο 17 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ. Τέλος, διά της προστασίας της ακεραιότητας των κρίσιμων υποδομών από κυβερνοεπιθέσεις, η πρόταση θα συμβάλει στο δικαίωμα στην προστασία της υγείας σύμφωνα με το άρθρο 35 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ και στο δικαίωμα πρόσβασης στις υπηρεσίες γενικού οικονομικού συμφέροντος σύμφωνα με το άρθρο 36 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ.

## 4. ΔΗΜΟΣΙΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ

Οι δράσεις του παρόντος κανονισμού θα στηριχθούν με χρηματοδότηση στο πλαίσιο του στρατηγικού στόχου «Κυβερνοασφάλεια» του προγράμματος «Ψηφιακή Ευρώπη».

Ο συνολικός προϋπολογισμός περιλαμβάνει αύξηση κατά 100 εκατ. EUR, η οποία προτείνεται στον παρόντα κανονισμό να κατανεμηθεί εκ νέου από άλλους στρατηγικούς στόχους του προγράμματος «Ψηφιακή Ευρώπη». Με τον τρόπο αυτό, το νέο συνολικό ποσό που διατίθεται για δράσεις κυβερνοασφάλειας στο πλαίσιο του προγράμματος «Ψηφιακή Ευρώπη» θα ανέλθει σε 842,8 εκατ. EUR.

Μέρος των πρόσθετων 100 εκατ. EUR θα ενισχύσει τον προϋπολογισμό που διαχειρίζεται το ECCC για την υλοποίηση δράσεων σχετικά με τα SOC και την ετοιμότητα στο πλαίσιο του/των προγράμματος/-ων εργασίας τους. Επιπλέον, η πρόσθετη χρηματοδότηση θα αξιοποιηθεί για τη στήριξη της δημιουργίας της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας.

Συμπληρώνει τον προϋπολογισμό που έχει ήδη προβλεφθεί για παρόμοιες δράσεις στο πλαίσιο του προγράμματος εργασίας του κύριου προγράμματος «Ψηφιακή Ευρώπη» και του προγράμματος εργασίας για την κυβερνοασφάλεια του προγράμματος «Ψηφιακή Ευρώπη» από την περίοδο 2023-2027, γεγονός που θα μπορούσε να αυξήσει το συνολικό ποσό σε 551 εκατομμύρια για την περίοδο 2023-2027, ενώ 115 εκατομμύρια διατέθηκαν ήδη με τη μορφή πιλοτικών έργων για την περίοδο 2021-2022. Συμπεριλαμβανομένων των συνεισφορών των κρατών μελών, ο συνολικός προϋπολογισμός μπορεί να ανέλθει σε 1 109 δισ. EUR.

Επισκόπηση του σχετικού κόστους περιλαμβάνεται στο «νομοθετικό δημοσιονομικό δελτίο» που συνοδεύει την παρούσα πρόταση.

## 5. ΛΟΙΠΑ ΣΤΟΙΧΕΙΑ

- **Σχέδια εφαρμογής και ρυθμίσεις παρακολούθησης, αξιολόγησης και υποβολής εκθέσεων**

Η Επιτροπή παρακολουθεί την υλοποίηση, την εφαρμογή και τη συμμόρφωση προς τις νέες αυτές διατάξεις με σκοπό την αξιολόγηση της αποτελεσματικότητάς τους. Η Επιτροπή υποβάλλει έκθεση σχετικά με την αξιολόγηση και την επανεξέταση του παρόντος κανονισμού στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο εντός τεσσάρων ετών από την ημερομηνία εφαρμογής του.

- **Αναλυτική επεξήγηση των επιμέρους διατάξεων της πρότασης**

Γενικοί στόχοι, αντικείμενο και ορισμοί (κεφάλαιο I)

Το κεφάλαιο I καθορίζει τους στόχους του κανονισμού για την ενίσχυση της αλληλεγγύης σε επίπεδο Ένωσης με σκοπό την καλύτερη ανίχνευση, προετοιμασία και αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας και, ειδικότερα, την ενίσχυση της κοινής ενωσιακής

ανίχνευσης και αντίληψης της κατάστασης όσον αφορά κυβερνοαπειλές και περιστατικά, την ενίσχυση της ετοιμότητας των οντοτήτων που δραστηριοποιούνται σε τομείς κρίσιμης και εξαιρετικά κρίσιμης σημασίας σε ολόκληρη την Ένωση και την ενίσχυση της αλληλεγγύης μέσω της ανάπτυξης κοινών ικανοτήτων αντιμετώπισης σημαντικών ή μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας και την ενίσχυση της ανθεκτικότητας της Ένωσης μέσω της επανεξέτασης και της αξιολόγησης σημαντικών ή μεγάλης κλίμακας περιστατικών. Το παρόν κεφάλαιο καθορίζει επίσης τις δράσεις μέσω των οποίων θα επιτευχθούν οι στόχοι αυτοί: ανάπτυξη ευρωπαϊκής κυβερνοασπίδας, δημιουργία μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο και δημιουργία μηχανισμού εξέτασης περιστατικών κυβερνοασφάλειας. Περιλαμβάνει επίσης τους ορισμούς που χρησιμοποιούνται σε όλη την έκταση της πράξης.

Η ευρωπαϊκή κυβερνοασπίδα (κεφάλαιο ΙΙ)

Το κεφάλαιο ΙΙ θεσπίζει την ευρωπαϊκή κυβερνοασπίδα και καθορίζει τα διάφορα στοιχεία της και τις προϋποθέσεις συμμετοχής. Πρώτον, εξαγγέλλει τον γενικό στόχο της ευρωπαϊκής κυβερνοασπίδας, ο οποίος συνίσταται στην ανάπτυξη προηγμένων ικανοτήτων της Ένωσης όσον αφορά την ανίχνευση, την ανάλυση και την επεξεργασία δεδομένων σχετικά με κυβερνοαπειλές και περιστατικά στην Ένωση, καθώς και τους ειδικούς επιχειρησιακούς στόχους. Ορίζει ότι η ενωσιακή χρηματοδότηση για την ευρωπαϊκή κυβερνοασπίδα υλοποιείται σύμφωνα με τον κανονισμό για το πρόγραμμα «Ψηφιακή Ευρώπη».

Επιπλέον, το κεφάλαιο περιγράφει τον τύπο οντοτήτων που θα συγκροτήσουν την ευρωπαϊκή κυβερνοασπίδα. Η ασπίδα αποτελείται από εθνικά κέντρα επιχειρήσεων ασφάλειας (στο εξής: εθνικά SOC) και διασυνοριακά κέντρα επιχειρήσεων ασφάλειας (στο εξής: διασυνοριακά SOC). Κάθε συμμετέχον κράτος μέλος ορίζει εθνικό SOC. Αυτό λειτουργεί ως σημείο αναφοράς και πύλη προς άλλους δημόσιους και ιδιωτικούς οργανισμούς σε εθνικό επίπεδο για τη συλλογή και ανάλυση πληροφοριών σχετικά με απειλές και περιστατικά κυβερνοασφάλειας και για τη συμβολή σε ένα διασυνοριακό SOC. Μετά από πρόσκληση εκδήλωσης ενδιαφέροντος, ένα εθνικό SOC μπορεί να επιλεγεί από το ECCC προκειμένου να συμμετάσχει σε κοινή διαδικασία προμηθειών εργαλείων και υποδομών με το ECCC και να λάβει επιχορήγηση για τη λειτουργία των εργαλείων και των υποδομών. Εάν ένα εθνικό SOC λαμβάνει στήριξη από την Ένωση, δεσμεύεται να υποβάλει αίτηση συμμετοχής σε διασυνοριακό SOC εντός δύο ετών.

Τα διασυνοριακά SOC συνίστανται σε μια κοινοπραξία τουλάχιστον τριών κρατών μελών, εκπροσωπούμενων από τα εθνικά SOC, τα οποία δεσμεύονται να συνεργάζονται για τον συντονισμό των δραστηριοτήτων τους για την ανίχνευση και την παρακολούθηση απειλών στον κυβερνοχώρο. Μετά από αρχική πρόσκληση εκδήλωσης ενδιαφέροντος, το ECCC μπορεί να επιλέξει κοινοπραξία υποδοχής για να συμμετάσχει σε κοινή προμήθεια εργαλείων και υποδομών με το ECCC και να λάβει επιχορήγηση για τη λειτουργία των εργαλείων και των υποδομών. Τα μέλη της κοινοπραξίας υποδοχής συνάπτουν γραπτή συμφωνία κοινοπραξίας στην οποία καθορίζονται οι εσωτερικές τους ρυθμίσεις. Στο παρόν κεφάλαιο αναλύονται στη συνέχεια οι απαιτήσεις για την ανταλλαγή πληροφοριών μεταξύ των συμμετεχόντων σε διασυνοριακό SOC και για την ανταλλαγή πληροφοριών μεταξύ ενός

διασυνοριακού SOC και άλλων διασυνοριακών SOC, καθώς και με τις σχετικές οντότητες της ΕΕ. Τα εθνικά SOC που συμμετέχουν σε διασυνοριακό SOC ανταλλάσσουν μεταξύ τους σχετικές πληροφορίες σχετικά με κυβερνοαπειλές, και οι λεπτομέρειες, συμπεριλαμβανομένης της δέσμευσης για ανταλλαγή σημαντικού όγκου δεδομένων και των σχετικών όρων, θα πρέπει να καθορίζονται σε συμφωνία κοινοπραξίας. Τα διασυνοριακά SOC εξασφαλίζουν υψηλό επίπεδο διαλειτουργικότητας μεταξύ τους. Τα διασυνοριακά SOC θα πρέπει επίσης να συνάπτουν συμφωνίες συνεργασίας με άλλα διασυνοριακά SOC, στις οποίες προσδιορίζονται οι αρχές ανταλλαγής πληροφοριών. Όταν τα διασυνοριακά SOC λαμβάνουν πληροφορίες σχετικά με δυνητικό ή εξελισσόμενο μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας, παρέχουν σχετικές πληροφορίες στο EU-CyCLONe, στο δίκτυο CSIRT και στην Επιτροπή, λαμβανομένων υπόψη των αντίστοιχων ρόλων τους όσον αφορά τη διαχείριση κρίσεων σύμφωνα με την οδηγία (ΕΕ) 2022/2555. Το κεφάλαιο ΙΙ ολοκληρώνεται με τον καθορισμό των όρων ασφάλειας για τη συμμετοχή στην ευρωπαϊκή κυβερνοασπίδα.

Μηχανισμός έκτακτης ανάγκης για την κυβερνοασφάλεια (κεφάλαιο ΙΙΙ)

Το κεφάλαιο ΙΙΙ θεσπίζει τον μηχανισμό έκτακτης ανάγκης στον κυβερνοχώρο με σκοπό τη βελτίωση της ανθεκτικότητας της Ένωσης σε μείζονες απειλές κυβερνοασφάλειας και την προετοιμασία και τον μετριασμό, σε πνεύμα αλληλεγγύης, των βραχυπρόθεσμων επιπτώσεων σημαντικών και μεγάλης κλίμακας περιστατικών ή κρίσεων στον τομέα της κυβερνοασφάλειας. Οι δράσεις για την υλοποίηση του μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο στηρίζονται μέσω χρηματοδότησης από το πρόγραμμα «Ψηφιακή Ευρώπη». Ο μηχανισμός προβλέπει δράσεις για τη στήριξη της ετοιμότητας, συμπεριλαμβανομένων συντονισμένων δοκιμών των οντοτήτων που δραστηριοποιούνται σε τομείς εξαιρετικά κρίσιμης σημασίας, της αντιμετώπισης και της άμεσης ανάκαμψης από σημαντικά ή μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας ή για τον μετριασμό των σημαντικών κυβερνοαπειλών και δράσεις αμοιβαίας συνδρομής.

Οι δράσεις ετοιμότητας του μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο περιλαμβάνουν τις συντονισμένες δοκιμές ετοιμότητας οντοτήτων που δραστηριοποιούνται σε τομείς εξαιρετικά κρίσιμης σημασίας. Η Επιτροπή, κατόπιν διαβούλευσης με τον ENISA και την ομάδα συνεργασίας NIS, θα πρέπει να προσδιορίζει τακτικά σχετικούς τομείς ή υποτομείς από τους τομείς υψηλής κρισιμότητας που απαριθμούνται στο παράρτημα Ι της οδηγίας (ΕΕ) 2022/2555, των οποίων οι οντότητες μπορούν να υπόκεινται σε συντονισμένες δοκιμές ετοιμότητας σε επίπεδο ΕΕ.

Για τους σκοπούς της υλοποίησης των προτεινόμενων δράσεων αντιμετώπισης περιστατικών, ο παρών κανονισμός θεσπίζει εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, η οποία αποτελείται από υπηρεσίες αντιμετώπισης περιστατικών από αξιόπιστους παρόχους, οι οποίοι επιλέγονται σύμφωνα με τα κριτήρια που καθορίζονται στον παρόντα κανονισμό. Οι χρήστες των υπηρεσιών από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας είναι οι αρχές διαχείρισης κρίσεων στον κυβερνοχώρο και οι CSIRT των κρατών μελών, καθώς και τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης. Η Επιτροπή έχει τη συνολική ευθύνη για την υλοποίηση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας και μπορεί να

αναθέσει στον ENISA, εν όλω ή εν μέρει, τη λειτουργία και τη διαχείριση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας.

Για να λάβουν στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, οι χρήστες θα πρέπει να λαμβάνουν τα δικά τους μέτρα για τον μετριασμό των επιπτώσεων του περιστατικού για το οποίο ζητείται η στήριξη. Τα αιτήματα στήριξης από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας θα πρέπει να περιλαμβάνουν τις απαραίτητες σχετικές πληροφορίες σχετικά με το περιστατικό και τα μέτρα που έχουν ήδη λάβει οι χρήστες. Το κεφάλαιο περιγράφει επίσης τις λεπτομέρειες υλοποίησης, συμπεριλαμβανομένης της αξιολόγησης των αιτημάτων για την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας.

Ο κανονισμός προβλέπει επίσης τις αρχές προμηθειών και τα κριτήρια επιλογής όσον αφορά τους αξιόπιστους παρόχους της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας.

Τρίτες χώρες μπορούν να ζητήσουν στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, εφόσον αυτό προβλέπεται από συμφωνίες σύνδεσης που έχουν συναφθεί σχετικά με τη συμμετοχή τους στο πρόγραμμα «Ψηφιακή Ευρώπη». Στο παρόν κεφάλαιο περιγράφονται περαιτέρω όροι και λεπτομέρειες της εν λόγω συμμετοχής.

Μηχανισμός εξέτασης περιστατικών κυβερνοασφάλειας (κεφάλαιο IV)

Κατόπιν αιτήματος της Επιτροπής, του EU-CyCLONe ή του δικτύου CSIRT, ο ENISA θα πρέπει να επανεξετάζει και να αξιολογεί απειλές, τρωτά σημεία και δράσεις μετριασμού σε σχέση με συγκεκριμένο σημαντικό ή μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας. Η επανεξέταση και η αξιολόγηση θα πρέπει να υποβάλλονται από τον ENISA με τη μορφή έκθεσης επανεξέτασης περιστατικού στο δίκτυο CSIRT, στο EU-CyCLONe και στην Επιτροπή, ώστε να υποστηρίζονται κατά την εκτέλεση των καθηκόντων τους. Όταν το περιστατικό αφορά τρίτη χώρα, η έκθεση θα πρέπει να κοινοποιείται από την Επιτροπή στον/στην ύπατο/-η εκπρόσωπο. Η έκθεση θα πρέπει να περιλαμβάνει τα διδάγματα που αντλήθηκαν και, κατά περίπτωση, συστάσεις για τη βελτίωση της στάσης της Ένωσης στον κυβερνοχώρο.

Τελικές διατάξεις (κεφάλαιο X)

Το κεφάλαιο V περιλαμβάνει τροποποιήσεις στον κανονισμό για το πρόγραμμα «Ψηφιακή Ευρώπη», καθώς και την υποχρέωση της Επιτροπής να εκπονεί και να υποβάλλει τακτικές εκθέσεις για την αξιολόγηση και την επανεξέταση του κανονισμού προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο. Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει εκτελεστικές πράξεις σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 21 με σκοπό: τον καθορισμό των προϋποθέσεων για την εν λόγω διαλειτουργικότητα μεταξύ των διασυνοριακών SOC· τον καθορισμό των διαδικαστικών ρυθμίσεων για την ανταλλαγή πληροφοριών σχετικά με δυνητικό ή εξελισσόμενο μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας μεταξύ διασυνοριακών SOC και οντοτήτων της Ένωσης· τον καθορισμό τεχνικών απαιτήσεων για τη διασφάλιση υψηλού επιπέδου δεδομένων και υλικής ασφάλειας της υποδομής και για την προστασία των συμφερόντων ασφάλειας της Ένωσης κατά την ανταλλαγή πληροφοριών με οντότητες που δεν είναι δημόσιοι φορείς των κρατών

μελών· τον προσδιορισμό των ειδών και του αριθμού των υπηρεσιών αντιμετώπισης που απαιτούνται για την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας· και τον περαιτέρω καθορισμό των λεπτομερών ρυθμίσεων για την κατανομή των υπηρεσιών υποστήριξης της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας.

2023/0109 (COD)

Πρόταση

# ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

## σχετικά με τον καθορισμό μέτρων για την ενίσχυση της αλληλεγγύης και των ικανοτήτων της Ένωσης για την ανίχνευση, την προετοιμασία και την αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας

ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ιδίως το άρθρο 173 παράγραφος 3 και το άρθρο 322 παράγραφος 1 στοιχείο α),

Έχοντας υπόψη την πρόταση της Ευρωπαϊκής Επιτροπής,

Κατόπιν διαβίβασης του σχεδίου νομοθετικής πράξης στα εθνικά κοινοβούλια,

Έχοντας υπόψη τη γνώμη του Ελεγκτικού Συνεδρίου[1],

Έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής[2],

Έχοντας υπόψη τη γνώμη της Επιτροπής των Περιφερειών[3],

Αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία,

Εκτιμώντας τα ακόλουθα:

(1) Η χρήση των τεχνολογιών πληροφοριών και επικοινωνιών και η εξάρτηση από αυτές είναι πλέον θεμελιώδεις πτυχές σε όλους τους τομείς της οικονομικής δραστηριότητας, καθώς οι δημόσιες διοικήσεις, οι εταιρείες μας και οι πολίτες είναι πιο διασυνδεδεμένοι και αλληλεξαρτώμενοι από ποτέ, πέρα από τομείς και σύνορα.

(2) Το μέγεθος, η συχνότητα και οι επιπτώσεις των περιστατικών κυβερνοασφάλειας αυξάνονται, συμπεριλαμβανομένων των επιθέσεων στην αλυσίδα εφοδιασμού με στόχο την κυβερνοκατασκοπεία, την εγκατάσταση λυτρισμικού ή την πρόκληση διαταραχών. Αποτελούν μείζονα απειλή για τη λειτουργία των συστημάτων δικτύου και πληροφοριών. Ενόψει του ταχέως εξελισσόμενου τοπίου των απειλών, η απειλή πιθανών περιστατικών μεγάλης κλίμακας που προκαλούν σημαντική διαταραχή ή ζημία σε κρίσιμες υποδομές απαιτεί αυξημένη ετοιμότητα σε όλα τα επίπεδα του πλαισίου κυβερνοασφάλειας της Ένωσης. Η απειλή αυτή υπερβαίνει τη στρατιωτική επίθεση της Ρωσίας κατά της Ουκρανίας και είναι πιθανό να συνεχίσει να υφίσταται, δεδομένης της πληθώρας των συνασπιζόμενων με το κράτος εγκληματικών παραγόντων και παραγόντων χακτιβισμού (ακτιβισμός στον κυβερνοχώρο) που εμπλέκονται στις τρέχουσες γεωπολιτικές εντάσεις. Τέτοια περιστατικά μπορούν να παρεμποδίσουν την παροχή δημόσιων υπηρεσιών και την άσκηση οικονομικών δραστηριοτήτων, μεταξύ άλλων σε τομείς κρίσιμης ή εξαιρετικά κρίσιμης σημασίας, να προκαλέσουν σημαντικές οικονομικές ζημίες, να υπονομεύσουν την εμπιστοσύνη

[1] ΕΕ C […] της […], σ. […].
[2] ΕΕ C της , σ .
[3] ΕΕ C της , σ .

των χρηστών, να προκαλέσουν σημαντική ζημία στην οικονομία της Ένωσης, και μπορούν ακόμη και να έχουν συνέπειες που απειλούν την υγεία ή τη ζωή. Επιπλέον, τα περιστατικά κυβερνοασφάλειας είναι απρόβλεπτα, καθώς συχνά εμφανίζονται και εξελίσσονται σε πολύ σύντομο χρονικό διάστημα, δεν περιορίζονται σε κάποια συγκεκριμένη γεωγραφική περιοχή και συμβαίνουν ταυτόχρονα ή εξαπλώνονται αμέσως σε πολλές χώρες.

(3) Είναι απαραίτητο να ενισχυθεί η ανταγωνιστική θέση των τομέων της βιομηχανίας και των υπηρεσιών στην Ένωση σε ολόκληρη την ψηφιοποιημένη οικονομία και να στηριχθεί ο ψηφιακός μετασχηματισμός τους, διά της ενίσχυσης του επιπέδου κυβερνοασφάλειας στην ψηφιακή ενιαία αγορά. Όπως συνιστάται σε τρεις διαφορετικές προτάσεις της Διάσκεψης για το μέλλον της Ευρώπης[4], είναι αναγκαίο να αυξηθεί η ανθεκτικότητα των πολιτών, των επιχειρήσεων και των οντοτήτων που διαχειρίζονται κρίσιμες υποδομές έναντι των αυξανόμενων απειλών κυβερνοασφάλειας, οι οποίες μπορούν να έχουν καταστροφικές κοινωνικές και οικονομικές επιπτώσεις. Ως εκ τούτου, απαιτούνται επενδύσεις σε υποδομές και υπηρεσίες που θα στηρίξουν την ταχύτερη ανίχνευση και αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας, και τα κράτη μέλη χρειάζονται βοήθεια για την καλύτερη προετοιμασία, καθώς και για την αντιμετώπιση σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας. Η Ένωση θα πρέπει επίσης να αυξήσει τις ικανότητές της σε αυτούς τους τομείς, ιδίως όσον αφορά τη συλλογή και ανάλυση δεδομένων σχετικά με απειλές και περιστατικά κυβερνοασφάλειας.

(4) Η Ένωση έχει ήδη λάβει σειρά μέτρων για τη μείωση των τρωτών σημείων και την αύξηση της ανθεκτικότητας των κρίσιμων υποδομών και οντοτήτων έναντι των κινδύνων κυβερνοασφάλειας, ιδίως με την οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[5], τη σύσταση (ΕΕ) 2017/1584 της Επιτροπής[6], την οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[7] και τον κανονισμό (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[8]. Επιπλέον, η σύσταση του Συμβουλίου σχετικά με μια συντονισμένη προσέγγιση σε επίπεδο Ένωσης για την ενίσχυση της ανθεκτικότητας των κρίσιμων υποδομών καλεί τα κράτη μέλη να λάβουν επείγοντα και αποτελεσματικά μέτρα και να συνεργαστούν καλόπιστα, αποδοτικά, με αλληλεγγύη και με συντονισμένο τρόπο μεταξύ τους, με την Επιτροπή και άλλες σχετικές δημόσιες αρχές, καθώς και με τις οικείες οντότητες,

---

4 https://futureu.europa.eu/el/

5 Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (ΕΕ L 333 της 27.12.2022, σ. 80).

6 Σύσταση (ΕΕ) 2017/1584 της Επιτροπής, της 13ης Σεπτεμβρίου 2017, για τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο (ΕΕ L 239 της 19.9.2017, σ. 36).

7 Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Αυγούστου 2013, για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου (ΕΕ L 218 της 14.8.2013, σ. 8).

8 Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια) (ΕΕ L 151 της 7.6.2019, σ. 15).

για την ενίσχυση της ανθεκτικότητας των κρίσιμων υποδομών που χρησιμοποιούνται για την παροχή βασικών υπηρεσιών στην εσωτερική αγορά.

(5) Οι αυξανόμενοι κίνδυνοι κυβερνοασφάλειας και ένα συνολικά σύνθετο τοπίο απειλών, με σαφή κίνδυνο ταχείας πρόκλησης δευτερογενών επιπτώσεων από τα περιστατικά στον κυβερνοχώρο από ένα κράτος μέλος σε άλλα και από τρίτη χώρα στην Ένωση, απαιτούν ενισχυμένη αλληλεγγύη σε επίπεδο Ένωσης για την καλύτερη ανίχνευση, προετοιμασία και αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας. Τα κράτη μέλη κάλεσαν επίσης την Επιτροπή να υποβάλει πρόταση σχετικά με ένα νέο ταμείο αντιμετώπισης καταστάσεων έκτακτης ανάγκης στον τομέα της κυβερνοασφάλειας στα συμπεράσματα του Συμβουλίου σχετικά με τη στάση της ΕΕ[9].

(6) Η κοινή ανακοίνωση σχετικά με την «Πολιτική της ΕΕ για την κυβερνοάμυνα»[10], που εκδόθηκε στις 10 Νοεμβρίου 2022, ανήγγειλε μια πρωτοβουλία αλληλεγγύης της ΕΕ στον κυβερνοχώρο με τους ακόλουθους στόχους: ενίσχυση των κοινών ικανοτήτων ανίχνευσης, αντίληψης της κατάστασης και αντίδρασης της ΕΕ μέσω της προώθησης της ανάπτυξης υποδομής κέντρων επιχειρήσεων ασφάλειας της ΕΕ (στο εξής: SOC), της στήριξης της σταδιακής δημιουργίας εφεδρείας στον τομέα της κυβερνοασφάλειας σε επίπεδο ΕΕ με υπηρεσίες από αξιόπιστους ιδιωτικούς παρόχους και της δοκιμής κρίσιμων οντοτήτων για πιθανά τρωτά σημεία με βάση εκτιμήσεις κινδύνου της ΕΕ.

(7) Είναι αναγκαίο να ενισχυθούν η ανίχνευση και η αντίληψη της κατάστασης όσον αφορά τις απειλές και τα περιστατικά στον κυβερνοχώρο σε ολόκληρη την Ένωση και να ενισχυθεί η αλληλεγγύη με την ενίσχυση της ετοιμότητας και των ικανοτήτων των κρατών μελών και της Ένωσης για την αντιμετώπιση σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας. Ως εκ τούτου, θα πρέπει να αναπτυχθεί πανευρωπαϊκή υποδομή SOC (ευρωπαϊκή κυβερνοασπίδα) για την οικοδόμηση και ενίσχυση κοινών ικανοτήτων ανίχνευσης και αντίληψης της κατάστασης· θα πρέπει να δημιουργηθεί μηχανισμός έκτακτης ανάγκης για την κυβερνοασφάλεια με σκοπό τη στήριξη των κρατών μελών όσον αφορά την προετοιμασία, την αντίδραση και την άμεση ανάκαμψη από σημαντικά και μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας· θα πρέπει να θεσπιστεί μηχανισμός εξέτασης περιστατικών κυβερνοασφάλειας για την εξέταση και την αξιολόγηση συγκεκριμένων σημαντικών ή μεγάλης κλίμακας περιστατικών. Οι εν λόγω δράσεις δεν θίγουν τα άρθρα 107 και 108 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (στο εξής: ΣΛΕΕ).

(8) Για την επίτευξη των στόχων αυτών, είναι επίσης αναγκαίο να τροποποιηθεί ο κανονισμός (ΕΕ) 2021/694 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[11] σε ορισμένους τομείς. Ειδικότερα, ο παρών κανονισμός θα πρέπει να τροποποιήσει τον κανονισμό (ΕΕ) 2021/694 όσον αφορά την προσθήκη νέων επιχειρησιακών στόχων που σχετίζονται με την ευρωπαϊκή κυβερνοασπίδα και τον μηχανισμό έκτακτης ανάγκης στον κυβερνοχώρο στο πλαίσιο του ειδικού στόχου 3 του προγράμματος

---

9 Συμπεράσματα του Συμβουλίου σχετικά με τη διαμόρφωση της στάσης της Ευρωπαϊκής Ένωσης στον κυβερνοχώρο, τα οποία εγκρίθηκαν από το Συμβούλιο κατά τη σύνοδό του στις 23 Μαΐου 2022 (9364/22).

10 Κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο «Πολιτική της ΕΕ για την κυβερνοάμυνα» [JOIN(2022) 49 final].

11 Κανονισμός (ΕΕ) 2021/694 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 29ης Απριλίου 2021, για τη θέσπιση του προγράμματος Ψηφιακή Ευρώπη και την κατάργηση της απόφασης (ΕΕ) 2015/2240 (ΕΕ L 166 της 11.5.2021, σ. 1).

«Ψηφιακή Ευρώπη», ο οποίος αποσκοπεί στη διασφάλιση της ανθεκτικότητας, της ακεραιότητας και της αξιοπιστίας της ψηφιακής ενιαίας αγοράς, στην ενίσχυση των ικανοτήτων παρακολούθησης των κυβερνοεπιθέσεων και απειλών και στην αντιμετώπιση αυτών, καθώς και στην ενίσχυση της διασυνοριακής συνεργασίας στον τομέα της κυβερνοασφάλειας. Τα παραπάνω θα συμπληρωθούν με τις ειδικές προϋποθέσεις υπό τις οποίες μπορεί να χορηγηθεί χρηματοδοτική στήριξη για τις εν λόγω δράσεις και θα πρέπει να καθοριστούν οι μηχανισμοί διακυβέρνησης και συντονισμού που απαιτούνται για την επίτευξη των επιδιωκόμενων στόχων. Άλλες τροποποιήσεις του κανονισμού (ΕΕ) 2021/694 θα πρέπει να περιλαμβάνουν περιγραφές των προτεινόμενων δράσεων στο πλαίσιο των νέων επιχειρησιακών στόχων, καθώς και μετρήσιμους δείκτες για την παρακολούθηση της υλοποίησης των εν λόγω νέων επιχειρησιακών στόχων.

(9) Η χρηματοδότηση των δράσεων στο πλαίσιο του παρόντος κανονισμού θα πρέπει να προβλέπεται στον κανονισμό (ΕΕ) 2021/694, ο οποίος θα πρέπει να εξακολουθήσει να αποτελεί τη συναφή βασική πράξη για τις εν λόγω δράσεις που προβλέπονται στον ειδικό στόχο 3 του προγράμματος «Ψηφιακή Ευρώπη». Οι ειδικές προϋποθέσεις συμμετοχής όσον αφορά κάθε δράση θα προβλέπονται στα σχετικά προγράμματα εργασίας, σύμφωνα με τις εφαρμοστέες διατάξεις του κανονισμού (ΕΕ) 2021/694.

(10) Οι οριζόντιοι δημοσιονομικοί κανόνες που εγκρίθηκαν από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο βάσει του άρθρου 322 ΣΛΕΕ έχουν εφαρμογή στον παρόντα κανονισμό. Οι κανόνες αυτοί καθορίζονται στον δημοσιονομικό κανονισμό και ρυθμίζουν ιδίως τις πρακτικές λεπτομέρειες κατάρτισης και εκτέλεσης του προϋπολογισμού της Ένωσης και οργανώνουν επίσης τον έλεγχο της ευθύνης των δημοσιονομικών φορέων. Οι κανόνες που θεσπίζονται βάσει του άρθρου 322 ΣΛΕΕ περιλαμβάνουν επίσης το γενικό καθεστώς αιρεσιμότητας για την προστασία του προϋπολογισμού της Ένωσης, όπως ορίζεται στον κανονισμό (ΕΕ, Ευρατόμ) 2020/2092 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

(11) Για τους σκοπούς της χρηστής δημοσιονομικής διαχείρισης, θα πρέπει να θεσπιστούν ειδικοί κανόνες για τη μεταφορά αχρησιμοποίητων πιστώσεων ανάληψης υποχρεώσεων και πιστώσεων πληρωμών. Τηρουμένης της αρχής ότι ο προϋπολογισμός της Ένωσης καθορίζεται ετησίως, ο παρών κανονισμός θα πρέπει, λόγω του απρόβλεπτου, έκτακτου και ειδικού χαρακτήρα του τοπίου της κυβερνοασφάλειας, να προβλέπει δυνατότητες μεταφοράς αχρησιμοποίητων κονδυλίων πέραν εκείνων που ορίζονται στον δημοσιονομικό κανονισμό, μεγιστοποιώντας έτσι την ικανότητα του μηχανισμού έκτακτης ανάγκης για την κυβερνοασφάλεια να στηρίζει τα κράτη μέλη όσον αφορά την αποτελεσματική αντιμετώπιση κυβερνοαπειλών.

(12) Για την αποτελεσματικότερη πρόληψη, αξιολόγηση και αντιμετώπιση κυβερνοαπειλών και περιστατικών, είναι αναγκαίο να αναπτυχθούν πληρέστερες γνώσεις σχετικά με τις απειλές κατά κρίσιμων πάγιων στοιχείων και υποδομών στο έδαφος της Ένωσης, συμπεριλαμβανομένης της γεωγραφικής κατανομής, της διασύνδεσης και των δυνητικών επιπτώσεών τους σε περίπτωση κυβερνοεπιθέσεων που επηρεάζουν τις εν λόγω υποδομές. Θα πρέπει να αναπτυχθεί μια μεγάλης κλίμακας ενωσιακή υποδομή SOC (στο εξής: ευρωπαϊκή κυβερνοασπίδα), η οποία θα αποτελείται από διάφορες διαλειτουργικές διασυνοριακές πλατφόρμες, καθεμία από τις οποίες θα συγκεντρώνει διάφορα εθνικά SOC. Οι εν λόγω υποδομές θα πρέπει να εξυπηρετούν εθνικά και ενωσιακά συμφέροντα και ανάγκες κυβερνοασφάλειας, αξιοποιώντας την τεχνολογία αιχμής για προηγμένα εργαλεία συλλογής και ανάλυσης δεδομένων, ενισχύοντας τις ικανότητες ανίχνευσης και διαχείρισης στον κυβερνοχώρο

και παρέχοντας αντίληψη της κατάστασης σε πραγματικό χρόνο. Οι υποδομές αυτές θα πρέπει να χρησιμεύουν για την αύξηση της ανίχνευσης απειλών και περιστατικών κυβερνοασφάλειας και, ως εκ τούτου, να συμπληρώνουν και να στηρίζουν τις οντότητες και τα δίκτυα της Ένωσης που είναι αρμόδια για τη διαχείριση κρίσεων στην Ένωση, ιδίως το δίκτυο οργανισμών διασύνδεσης για κυβερνοκρίσεις της ΕΕ (στο εξής: EU-CyCLONe), όπως ορίζεται στην οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[12].

(13) Κάθε κράτος μέλος θα πρέπει να ορίσει έναν δημόσιο φορέα σε εθνικό επίπεδο επιφορτισμένο με τον συντονισμό των δραστηριοτήτων ανίχνευσης κυβερνοαπειλών στο εν λόγω κράτος μέλος. Τα εν λόγω εθνικά SOC θα πρέπει να λειτουργούν ως σημείο αναφοράς και πύλη σε εθνικό επίπεδο για τη συμμετοχή στην ευρωπαϊκή κυβερνοασπίδα και θα πρέπει να διασφαλίζουν ότι οι πληροφορίες σχετικά με τις κυβερνοαπειλές από δημόσιους και ιδιωτικούς φορείς ανταλλάσσονται και συλλέγονται σε εθνικό επίπεδο με αποτελεσματικό και εξορθολογισμένο τρόπο.

(14) Στο πλαίσιο της ευρωπαϊκής κυβερνοασπίδας, θα πρέπει να συσταθούν ορισμένα διασυνοριακά κέντρα επιχειρήσεων κυβερνοασφάλειας (στο εξής: διασυνοριακά SOC). Σε αυτά θα πρέπει να συμμετέχουν εθνικά SOC από τουλάχιστον τρία κράτη μέλη, ώστε να μπορούν να επιτευχθούν πλήρως τα οφέλη της διασυνοριακής ανίχνευσης απειλών και της ανταλλαγής και διαχείρισης πληροφοριών. Γενικός στόχος των διασυνοριακών SOC θα πρέπει να είναι η ενίσχυση των ικανοτήτων ανάλυσης, πρόληψης και ανίχνευσης απειλών κυβερνοασφάλειας και η υποστήριξη της παραγωγής υψηλής ποιότητας πληροφοριών σχετικά με τις απειλές κυβερνοασφάλειας, ιδίως μέσω της ανταλλαγής δεδομένων από διάφορες πηγές, δημόσιες ή ιδιωτικές, καθώς και μέσω της ανταλλαγής και της κοινής χρήσης εργαλείων αιχμής και της από κοινού ανάπτυξης ικανοτήτων ανίχνευσης, ανάλυσης και πρόληψης σε ένα αξιόπιστο περιβάλλον. Θα πρέπει να παρέχουν νέα πρόσθετη ικανότητα, αξιοποιώντας και συμπληρώνοντας τα υφιστάμενα SOC και τις ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (στο εξής: CSIRT) και άλλους σχετικούς παράγοντες.

(15) Σε εθνικό επίπεδο, η παρακολούθηση, η ανίχνευση και η ανάλυση των κυβερνοαπειλών διασφαλίζεται συνήθως από τα SOC δημόσιων και ιδιωτικών οντοτήτων, σε συνδυασμό με τις CSIRT. Επιπλέον, οι CSIRT ανταλλάσσουν πληροφορίες στο πλαίσιο του δικτύου CSIRT, σύμφωνα με την οδηγία (ΕΕ) 2022/2555. Τα διασυνοριακά SOC θα πρέπει να αποτελέσουν μια νέα ικανότητα που θα συμπληρώνει το δίκτυο CSIRT, συγκεντρώνοντας και ανταλλάσσοντας δεδομένα σχετικά με απειλές κυβερνοασφάλειας από δημόσιες και ιδιωτικές οντότητες, ενισχύοντας την αξία των εν λόγω δεδομένων μέσω αναλύσεων εμπειρογνωμόνων και από κοινού αποκτηθεισών υποδομών και εργαλείων αιχμής και συμβάλλοντας στην ανάπτυξη των ικανοτήτων και της τεχνολογικής κυριαρχίας της Ένωσης.

(16) Τα διασυνοριακά SOC θα πρέπει να λειτουργούν ως κεντρικό σημείο που επιτρέπει την ευρεία συγκέντρωση σχετικών δεδομένων και πληροφοριών για κυβερνοαπειλές, να καθιστούν δυνατή τη διάδοση πληροφοριών σχετικά με απειλές σε ένα ευρύ και ποικίλο σύνολο παραγόντων [π.χ. ομάδες αντιμετώπισης καταστάσεων έκτακτης

[12] Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2) (ΕΕ L 333 της 27.12.2022, σ. 80).

ανάγκης σε υπολογιστές (στο εξής: CERT), CSIRT, κέντρα ανταλλαγής και ανάλυσης πληροφοριών (στο εξής: ISAC), φορείς εκμετάλλευσης κρίσιμων υποδομών]. Οι πληροφορίες που ανταλλάσσονται μεταξύ των συμμετεχόντων σε ένα διασυνοριακό SOC μπορούν να περιλαμβάνουν δεδομένα από δίκτυα και αισθητήρες, ροές πληροφοριών σχετικά με απειλές, ενδείξεις της παραβίασης και εντός πλαισίου πληροφορίες σχετικά με περιστατικά, απειλές και τρωτά σημεία. Επιπλέον, τα διασυνοριακά SOC θα πρέπει επίσης να συνάπτουν συμφωνίες συνεργασίας με άλλα διασυνοριακά SOC.

(17) Η κοινή αντίληψη της κατάστασης μεταξύ των αρμόδιων αρχών αποτελεί απαραίτητη προϋπόθεση για την ετοιμότητα και τον συντονισμό σε επίπεδο Ένωσης όσον αφορά σημαντικά και μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας. Η οδηγία (ΕΕ) 2022/2555 συστήνει το EU-CyCLONe για να στηρίζει τη συντονισμένη διαχείριση μεγάλης κλίμακας περιστατικών και κρίσεων στον τομέα της κυβερνοασφάλειας σε επιχειρησιακό επίπεδο και να διασφαλίζει την τακτική ανταλλαγή σχετικών πληροφοριών μεταξύ των κρατών μελών και των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης. Η σύσταση (ΕΕ) 2017/1584 για τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο πραγματεύεται τον ρόλο όλων των σχετικών φορέων. Η οδηγία (ΕΕ) 2022/2555 υπενθυμίζει επίσης τις αρμοδιότητες της Επιτροπής στο πλαίσιο του μηχανισμού πολιτικής προστασίας της Ένωσης (στο εξής: ΜΠΠΕ) που θεσπίστηκε με την απόφαση 1313/2013/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, καθώς και όσον αφορά την υποβολή αναλυτικών εκθέσεων για τις ρυθμίσεις για τον μηχανισμό ολοκληρωμένης αντιμετώπισης πολιτικών κρίσεων της ΕΕ (στο εξής: IPCR) βάσει της εκτελεστικής απόφασης (ΕΕ) 2018/1993. Ως εκ τούτου, σε περιπτώσεις όπου τα διασυνοριακά SOC λαμβάνουν πληροφορίες σχετικά με πιθανό ή εξελισσόμενο μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας, θα πρέπει να παρέχουν σχετικές πληροφορίες στο EU-CyCLONe, στο δίκτυο CSIRT και στην Επιτροπή. Ειδικότερα, ανάλογα με την κατάσταση, οι πληροφορίες που πρέπει να ανταλλάσσονται θα μπορούσαν να περιλαμβάνουν τεχνικές πληροφορίες, πληροφορίες σχετικά με τη φύση και τα κίνητρα του δράστη της επίθεσης ή του δυνητικού δράστη της επίθεσης, καθώς και μη τεχνικές πληροφορίες υψηλότερου επιπέδου σχετικά με δυνητικό ή εξελισσόμενο μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας. Στο πλαίσιο αυτό, θα πρέπει να λαμβάνεται δεόντως υπόψη η αρχή της ανάγκης για γνώση και ο δυνητικά ευαίσθητος χαρακτήρας των πληροφοριών που ανταλλάσσονται.

(18) Οι οντότητες που συμμετέχουν στην ευρωπαϊκή κυβερνοασπίδα θα πρέπει να διασφαλίζουν υψηλό επίπεδο διαλειτουργικότητας μεταξύ τους, μεταξύ άλλων, κατά περίπτωση, όσον αφορά τους μορφότυπους δεδομένων, την ταξινόμηση, τα εργαλεία διαχείρισης και ανάλυσης δεδομένων και τους ασφαλείς διαύλους επικοινωνίας, ένα ελάχιστο επίπεδο ασφάλειας εφαρμογής, πίνακα εργαλείων αντίληψης της κατάστασης και δείκτες. Η θέσπιση κοινής ταξινόμησης και η ανάπτυξη υποδείγματος για τις εκθέσεις κατάστασης με σκοπό την περιγραφή της τεχνικής αιτίας και των επιπτώσεων των περιστατικών κυβερνοασφάλειας θα πρέπει να λαμβάνουν υπόψη τις συνεχιζόμενες εργασίες για την κοινοποίηση περιστατικών στο πλαίσιο της εφαρμογής της οδηγίας (ΕΕ) 2022/2555.

(19) Προκειμένου να καταστεί δυνατή η ανταλλαγή δεδομένων σχετικά με απειλές κυβερνοασφάλειας από διάφορες πηγές, σε ευρεία κλίμακα και σε ένα αξιόπιστο περιβάλλον, οι οντότητες που συμμετέχουν στην ευρωπαϊκή κυβερνοασπίδα θα πρέπει να είναι εφοδιασμένες με προηγμένα και υψηλής ασφάλειας εργαλεία, εξοπλισμό και

υποδομές. Με τον τρόπο αυτό θα καταστεί δυνατή η βελτίωση των συλλογικών ικανοτήτων ανίχνευσης και των έγκαιρων προειδοποιήσεων προς τις αρχές και τις σχετικές οντότητες, ιδίως με τη χρήση των πλέον πρόσφατων τεχνολογιών τεχνητής νοημοσύνης και ανάλυσης δεδομένων.

(20) Με τη συλλογή, την κοινοποίηση και την ανταλλαγή δεδομένων, η ευρωπαϊκή κυβερνοασπίδα θα πρέπει να ενισχύσει την τεχνολογική κυριαρχία της Ένωσης. Η συγκέντρωση επιμελημένων δεδομένων υψηλής ποιότητας θα πρέπει επίσης να συμβάλει στην ανάπτυξη προηγμένων τεχνολογιών τεχνητής νοημοσύνης και ανάλυσης δεδομένων. Η εν λόγω συγκέντρωση θα πρέπει να διευκολυνθεί μέσω της σύνδεσης της ευρωπαϊκής κυβερνοασπίδας με την πανευρωπαϊκή υποδομή υπολογιστικής υψηλών επιδόσεων που θεσπίστηκε με τον κανονισμό (ΕΕ) 2021/1173 του Συμβουλίου[13].

(21) Ενώ η ευρωπαϊκή κυβερνοασπίδα είναι ένα μη στρατιωτικό έργο, η κοινότητα κυβερνοάμυνας μπορεί να επωφεληθεί από ισχυρότερες μη στρατιωτικές ικανότητες ανίχνευσης και αντίληψης της κατάστασης που αναπτύχθηκαν για την προστασία κρίσιμων υποδομών. Τα διασυνοριακά SOC, με την υποστήριξη της Επιτροπής και του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας (στο εξής: ECCC), και σε συνεργασία με τον/την ύπατο/-η εκπρόσωπο της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας (στο εξής: ύπατος/-η εκπρόσωπος), θα πρέπει σταδιακά να αναπτύξουν ειδικά πρωτόκολλα και πρότυπα που θα επιτρέπουν τη συνεργασία με την κοινότητα κυβερνοάμυνας, συμπεριλαμβανομένων των όρων ελέγχου και ασφάλειας. Η ανάπτυξη της ευρωπαϊκής κυβερνοασπίδας θα πρέπει να συνοδεύεται από προβληματισμό που θα επιτρέπει τη μελλοντική συνεργασία με δίκτυα και πλατφόρμες ανταλλαγής πληροφοριών στην κοινότητα κυβερνοάμυνας, σε στενή συνεργασία με τον/την ύπατο/-η εκπρόσωπο.

(22) Η ανταλλαγή πληροφοριών μεταξύ των συμμετεχόντων στην ευρωπαϊκή κυβερνοασπίδα θα πρέπει να συμμορφώνεται με τις ισχύουσες νομικές απαιτήσεις, ιδίως δε με το ενωσιακό και το εθνικό δίκαιο για την προστασία των δεδομένων, καθώς και με τους ενωσιακούς κανόνες περί ανταγωνισμού που διέπουν την ανταλλαγή πληροφοριών. Ο αποδέκτης των πληροφοριών θα πρέπει να εφαρμόζει, στον βαθμό που είναι αναγκαία η επεξεργασία δεδομένων προσωπικού χαρακτήρα, τεχνικά και οργανωτικά μέτρα που διασφαλίζουν τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, να καταστρέφει τα δεδομένα μόλις παύσουν να είναι απαραίτητα για τον δηλωθέντα σκοπό και να ενημερώνει τον φορέα που καθιστά τα δεδομένα διαθέσιμα ότι τα δεδομένα έχουν καταστραφεί.

(23) Με την επιφύλαξη του άρθρου 346 ΣΛΕΕ, η ανταλλαγή εμπιστευτικών πληροφοριών δυνάμει ενωσιακών ή εθνικών κανόνων θα πρέπει να περιορίζεται σε ό,τι είναι συναφές και αναλογικό προς τον σκοπό της εν λόγω ανταλλαγής. Η ανταλλαγή των εν λόγω πληροφοριών θα πρέπει να διαφυλάσσει την εμπιστευτικότητα των πληροφοριών και να προστατεύει την ασφάλεια και τα εμπορικά συμφέροντα των οικείων οντοτήτων, με πλήρη σεβασμό του εμπορικού και επιχειρηματικού απορρήτου.

[13] Κανονισμός (ΕΕ) 2021/1173 του Συμβουλίου, της 13ης Ιουλίου 2021, σχετικά με τη σύσταση της κοινής επιχείρησης για την ευρωπαϊκή υπολογιστική υψηλών επιδόσεων και σχετικά με την κατάργηση του κανονισμού (ΕΕ) 2018/1488 (ΕΕ L 256 της 19.7.2021, σ. 3).

(24) Λαμβανομένων υπόψη των αυξανόμενων κινδύνων και του αριθμού των περιστατικών στον κυβερνοχώρο που επηρεάζουν τα κράτη μέλη, είναι αναγκαίο να δημιουργηθεί ένα μέσο στήριξης κρίσεων για τη βελτίωση της ανθεκτικότητας της Ένωσης σε σημαντικά και μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας και τη συμπλήρωση των δράσεων των κρατών μελών μέσω χρηματοδοτικής στήριξης έκτακτης ανάγκης της ετοιμότητας, της αντίδρασης και της άμεσης ανάκαμψης βασικών υπηρεσιών. Το μέσο αυτό θα πρέπει να επιτρέπει την ταχεία παροχή βοήθειας σε συγκεκριμένες περιστάσεις και υπό σαφείς προϋποθέσεις και να επιτρέπει την προσεκτική παρακολούθηση και αξιολόγηση του τρόπου με τον οποίο χρησιμοποιήθηκαν οι πόροι. Ενώ η πρόληψη, η ετοιμότητα και η αντιμετώπιση περιστατικών και κρίσεων κυβερνοασφάλειας είναι πρωτίστως ευθύνη των κρατών μελών, ο μηχανισμός έκτακτης ανάγκης στον κυβερνοχώρο προωθεί την αλληλεγγύη μεταξύ των κρατών μελών σύμφωνα με το άρθρο 3 παράγραφος 3 της Συνθήκης για την Ευρωπαϊκή Ένωση (στο εξής: ΣΕΕ).

(25) Ο μηχανισμός έκτακτης ανάγκης στον κυβερνοχώρο θα πρέπει να παρέχει στήριξη στα κράτη μέλη συμπληρώνοντας τα μέτρα και τους πόρους τους, καθώς και άλλες υφιστάμενες επιλογές στήριξης σε περίπτωση αντιμετώπισης σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας και άμεσης ανάκαμψης από αυτά, όπως οι υπηρεσίες που παρέχονται από τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (στο εξής: ENISA) στο πλαίσιο των αρμοδιοτήτων του, η συντονισμένη αντίδραση και συνδρομή από το δίκτυο CSIRT, η στήριξη μετριασμού από το EU-CyCLONe, καθώς και η αμοιβαία συνδρομή μεταξύ των κρατών μελών, μεταξύ άλλων στο πλαίσιο του άρθρου 42 παράγραφος 7 ΣΕΕ, οι ομάδες ταχείας αντίδρασης στον κυβερνοχώρο[14] και οι υβριδικές ομάδες ταχείας αντίδρασης της μόνιμης διαρθρωμένης συνεργασίας (PESCO). Θα πρέπει να αντιμετωπίσει την ανάγκη να διασφαλιστεί η διαθεσιμότητα εξειδικευμένων μέσων για τη στήριξη της ετοιμότητας και της αντιμετώπισης περιστατικών κυβερνοασφάλειας σε ολόκληρη την Ένωση και σε τρίτες χώρες.

(26) Το παρόν μέσο δεν θίγει τις διαδικασίες και τα πλαίσια για τον συντονισμό της αντιμετώπισης κρίσεων σε επίπεδο Ένωσης, ιδίως τον ΜΠΠΕ[15], τον IPCR[16],, και την οδηγία (ΕΕ) 2022/2555. Μπορεί να συμβάλλει ή να συμπληρώνει δράσεις που υλοποιούνται στο πλαίσιο του άρθρου 42 παράγραφος 7 ΣΕΕ ή σε καταστάσεις που ορίζονται στο άρθρο 222 ΣΛΕΕ. Η χρήση του εν λόγω μέσου θα πρέπει επίσης να συντονίζεται με την εφαρμογή των μέτρων της εργαλειοθήκης για τη διπλωματία στον κυβερνοχώρο, κατά περίπτωση.

(27) Η βοήθεια που παρέχεται δυνάμει του παρόντος κανονισμού θα πρέπει να στηρίζει και να συμπληρώνει τις δράσεις που αναλαμβάνουν τα κράτη μέλη σε εθνικό επίπεδο. Για τον σκοπό αυτό, θα πρέπει να εξασφαλίζεται στενή συνεργασία και διαβούλευση μεταξύ της Επιτροπής και του επηρεαζόμενου κράτους μέλους. Όταν ζητεί στήριξη

---

14 Απόφαση (ΚΕΠΠΑ) 2017/2315 του Συμβουλίου, της 11ης Δεκεμβρίου 2017, για τη θεσμοθέτηση μόνιμης διαρθρωμένης συνεργασίας (PESCO) και την κατάρτιση του καταλόγου των συμμετεχόντων κρατών μελών.

15 Απόφαση αριθ. 1313/2013/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Δεκεμβρίου 2013, περί μηχανισμού πολιτικής προστασίας της Ένωσης (ΕΕ L 347 της 20.12.2013, σ. 924).

16 Ρυθμίσεις ολοκληρωμένης αντιμετώπισης πολιτικών κρίσεων (IPCR) και σύμφωνα με τη σύσταση (ΕΕ) 2017/1584 της Επιτροπής, της 13ης Σεπτεμβρίου 2017, για τη συντονισμένη αντιμετώπιση μεγάλης κλίμακας περιστατικών και κρίσεων στον κυβερνοχώρο.

στο πλαίσιο του μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο, το κράτος μέλος θα πρέπει να παρέχει σχετικές πληροφορίες που αιτιολογούν την ανάγκη στήριξης.

(28) Η οδηγία (ΕΕ) 2022/2555 απαιτεί από τα κράτη μέλη να ορίσουν ή να συστήσουν μία ή περισσότερες αρχές διαχείρισης κυβερνοκρίσεων και να διασφαλίσουν ότι διαθέτουν επαρκείς πόρους για να επιτελούν αποτελεσματικά και αποδοτικά τα καθήκοντά τους. Απαιτεί επίσης από τα κράτη μέλη να προσδιορίζουν τις ικανότητες, τα πάγια στοιχεία και τις διαδικασίες που μπορούν να χρησιμοποιηθούν στην περίπτωση κρίσης καθώς και να θεσπίζουν εθνικό σχέδιο αντιμετώπισης περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας, στο οποίο καθορίζονται οι στόχοι και οι ρυθμίσεις για τη διαχείριση περιστατικών μεγάλης κλίμακας και κρίσεων στον τομέα της κυβερνοασφάλειας. Τα κράτη μέλη υποχρεούνται επίσης να συστήσουν μία ή περισσότερες CSIRT που είναι υπεύθυνες για τον χειρισμό περιστατικών σύμφωνα με σαφώς καθορισμένη διαδικασία και να καλύπτουν τουλάχιστον τους τομείς, υποτομείς και τύπους οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής της εν λόγω οδηγίας, και να διασφαλίζουν ότι διαθέτουν επαρκείς πόρους για να επιτελούν αποτελεσματικά τα καθήκοντά τους. Ο παρών κανονισμός δεν θίγει τον ρόλο της Επιτροπής όσον αφορά τη διασφάλιση της συμμόρφωσης των κρατών μελών προς τις υποχρεώσεις που απορρέουν από την οδηγία (ΕΕ) 2022/2555. Ο μηχανισμός έκτακτης ανάγκης στον κυβερνοχώρο θα πρέπει να παρέχει βοήθεια για δράσεις που αποσκοπούν στην ενίσχυση της ετοιμότητας, καθώς και για δράσεις αντιμετώπισης περιστατικών με σκοπό τον μετριασμό των επιπτώσεων σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας, τη στήριξη της άμεσης ανάκαμψης και/ή την αποκατάσταση της λειτουργίας βασικών υπηρεσιών.

(29) Στο πλαίσιο των δράσεων ετοιμότητας, για την προώθηση συνεκτικής προσέγγισης και την ενίσχυση της ασφάλειας σε ολόκληρη την Ένωση και την εσωτερική αγορά της, θα πρέπει να παρέχεται στήριξη για τη δοκιμή και την αξιολόγηση της κυβερνοασφάλειας οντοτήτων που δραστηριοποιούνται σε τομείς εξαιρετικά κρίσιμης σημασίας οι οποίοι προσδιορίζονται σύμφωνα με την οδηγία (ΕΕ) 2022/2555 με συντονισμένο τρόπο. Για τον σκοπό αυτό, η Επιτροπή, με την υποστήριξη του ENISA και σε συνεργασία με την ομάδα συνεργασίας NIS που συστάθηκε με την οδηγία (ΕΕ) 2022/2555, θα πρέπει να προσδιορίζει τακτικά σχετικούς τομείς ή υποτομείς, οι οποίοι θα πρέπει να είναι επιλέξιμοι για χρηματοδοτική στήριξη για συντονισμένες δοκιμές σε επίπεδο Ένωσης. Οι τομείς ή υποτομείς θα πρέπει να επιλέγονται από το παράρτημα Ι της οδηγίας (ΕΕ) 2022/2555 (στο εξής: τομείς υψηλής κρισιμότητας). Οι συντονισμένες δοκιμές θα πρέπει να βασίζονται σε κοινά σενάρια και μεθοδολογίες κινδύνου. Κατά την επιλογή των τομέων και την ανάπτυξη σεναρίων κινδύνου θα πρέπει να λαμβάνονται υπόψη οι σχετικές εκτιμήσεις κινδύνου και τα σενάρια κινδύνου σε επίπεδο Ένωσης, συμπεριλαμβανομένης της ανάγκης αποφυγής επικαλύψεων, όπως η εκτίμηση κινδύνου και τα σενάρια κινδύνου που απαιτούνται στα συμπεράσματα του Συμβουλίου σχετικά με τη διαμόρφωση της στάσης της Ευρωπαϊκής Ένωσης στον κυβερνοχώρο που διενεργεί/εκπονεί η Επιτροπή, ο/η ύπατος/-η εκπρόσωπος και η ομάδα συνεργασίας NIS, σε συντονισμό με τους αρμόδιους μη στρατιωτικούς και στρατιωτικούς φορείς και οργανισμούς και τα δημιουργηθέντα δίκτυα, συμπεριλαμβανομένου του EU-CyCLONe, καθώς και η εκτίμηση κινδύνου των δικτύων και υποδομών επικοινωνιών που ζητείται από την κοινή υπουργική έκκληση της Nevers και διενεργείται από την ομάδα συνεργασίας NIS, με την υποστήριξη της Επιτροπής και του ENISA, και σε συνεργασία με τον Φορέα Ευρωπαϊκών Ρυθμιστικών Αρχών για τις Ηλεκτρονικές Επικοινωνίες (BEREC), οι συντονισμένες εκτιμήσεις κινδύνου που πρέπει να διενεργούνται

σύμφωνα με το άρθρο 22 της οδηγίας (ΕΕ) 2022/2555 και οι δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας, όπως προβλέπεται στον κανονισμό (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[17]. Κατά την επιλογή των τομέων θα πρέπει επίσης να λαμβάνεται υπόψη η σύσταση του Συμβουλίου σχετικά με συντονισμένη προσέγγιση σε επίπεδο Ένωσης με σκοπό την ενίσχυση της ανθεκτικότητας των κρίσιμων υποδομών.

(30) Επιπλέον, ο μηχανισμός έκτακτης ανάγκης στον κυβερνοχώρο θα πρέπει να παρέχει στήριξη για άλλες δράσεις ετοιμότητας και να στηρίζει την ετοιμότητα σε άλλους τομείς, οι οποίοι δεν καλύπτονται από τις συντονισμένες δοκιμές οντοτήτων που δραστηριοποιούνται σε τομείς εξαιρετικά κρίσιμης σημασίας. Οι δράσεις αυτές μπορούν να περιλαμβάνουν διάφορα είδη εθνικών δραστηριοτήτων ετοιμότητας.

(31) Ο μηχανισμός έκτακτης ανάγκης στον κυβερνοχώρο θα πρέπει να παρέχει επίσης βοήθεια για δράσεις αντιμετώπισης περιστατικών με σκοπό τον μετριασμό των επιπτώσεων σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας, τη στήριξη της άμεσης ανάκαμψης και/ή την αποκατάσταση της λειτουργίας βασικών υπηρεσιών. Κατά περίπτωση, θα πρέπει να συμπληρώνει τον ΜΠΠΕ ώστε να διασφαλίζεται η ολοκληρωμένη προσέγγιση της αντιμετώπισης των επιπτώσεων των περιστατικών στον κυβερνοχώρο στους πολίτες.

(32) Ο μηχανισμός έκτακτης ανάγκης στον κυβερνοχώρο θα πρέπει να στηρίζει τη βοήθεια που παρέχεται από τα κράτη μέλη σε κράτος μέλος που επηρεάζεται από σημαντικό ή μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας, μεταξύ άλλων από το δίκτυο CSIRT που ορίζεται στο άρθρο 15 της οδηγίας (ΕΕ) 2022/2555. Τα κράτη μέλη που παρέχουν συνδρομή θα πρέπει να έχουν τη δυνατότητα να υποβάλλουν αιτήσεις για την κάλυψη των δαπανών που σχετίζονται με την αποστολή ομάδων εμπειρογνωμόνων στο πλαίσιο της αμοιβαίας συνδρομής. Οι επιλέξιμες δαπάνες μπορούν να περιλαμβάνουν έξοδα ταξιδίου, διαμονής και ημερήσιας αποζημίωσης των εμπειρογνωμόνων κυβερνοασφάλειας.

(33) Θα πρέπει σταδιακά να δημιουργηθεί εφεδρεία στον τομέα της κυβερνοασφάλειας σε επίπεδο Ένωσης, η οποία θα αποτελείται από υπηρεσίες από ιδιωτικούς παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας για την υποστήριξη δράσεων αντιμετώπισης και άμεσης ανάκαμψης σε περιπτώσεις σημαντικών ή μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας. Η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας θα πρέπει να διασφαλίζει τη διαθεσιμότητα και την ετοιμότητα των υπηρεσιών. Οι υπηρεσίες από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας θα πρέπει να χρησιμοποιούνται για τη στήριξη των εθνικών αρχών όσον αφορά την παροχή βοήθειας σε επηρεαζόμενες οντότητες που δραστηριοποιούνται σε τομείς κρίσιμης ή εξαιρετικά κρίσιμης σημασίας, συμπληρωματικά προς τις δικές τους δράσεις σε εθνικό επίπεδο. Όταν ζητούν στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, τα κράτη μέλη θα πρέπει να προσδιορίζουν τη στήριξη που παρέχεται στην πληγείσα οντότητα σε εθνικό επίπεδο, η οποία θα πρέπει να λαμβάνεται υπόψη κατά την αξιολόγηση του αιτήματος του κράτους μέλους. Οι υπηρεσίες από την εφεδρεία της ΕΕ στον τομέα της

[17] Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011.

κυβερνοασφάλειας μπορούν επίσης να χρησιμεύσουν για τη στήριξη των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης, υπό παρόμοιες συνθήκες.

(34) Για τους σκοπούς της επιλογής ιδιωτικών παρόχων υπηρεσιών για την παροχή υπηρεσιών στο πλαίσιο της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, είναι αναγκαίο να θεσπιστεί ένα σύνολο ελάχιστων κριτηρίων που θα πρέπει να περιλαμβάνονται στην πρόσκληση υποβολής προσφορών για την επιλογή των εν λόγω παρόχων, ώστε να διασφαλίζεται η κάλυψη των αναγκών των αρχών και των οντοτήτων των κρατών μελών που δραστηριοποιούνται σε τομείς κρίσιμης ή εξαιρετικά κρίσιμης σημασίας.

(35) Για τη στήριξη της δημιουργίας της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, η Επιτροπή μπορεί να εξετάσει το ενδεχόμενο να ζητήσει από τον ENISA να καταρτίσει υποψήφιο σύστημα πιστοποίησης σύμφωνα με τον κανονισμό (ΕΕ) 2019/881 για τις διαχειριζόμενες υπηρεσίες ασφάλειας στους τομείς που καλύπτονται από τον μηχανισμό έκτακτης ανάγκης στον κυβερνοχώρο.

(36) Προκειμένου να υποστηριχθούν οι στόχοι του παρόντος κανονισμού για την προώθηση της κοινής αντίληψης της κατάστασης, την ενίσχυση της ανθεκτικότητας της Ένωσης και τη διευκόλυνση της αποτελεσματικής αντιμετώπισης σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας, το EU-CyCLONe, το δίκτυο CSIRT ή η Επιτροπή θα πρέπει να είναι σε θέση να ζητούν από τον ENISA να εξετάζει και να αξιολογεί απειλές, τρωτά σημεία και δράσεις μετριασμού σε σχέση με συγκεκριμένο σημαντικό ή μεγάλης κλίμακας περιστατικό κυβερνοασφάλειας. Μετά την ολοκλήρωση της εξέτασης και της αξιολόγησης ενός περιστατικού, ο ENISA θα πρέπει να συντάσσει έκθεση εξέτασης περιστατικού, σε συνεργασία με τα σχετικά ενδιαφερόμενα μέρη, συμπεριλαμβανομένων εκπροσώπων του ιδιωτικού τομέα, των κρατών μελών, της Επιτροπής και άλλων σχετικών θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ. Όσον αφορά τον ιδιωτικό τομέα, ο ENISA αναπτύσσει διαύλους ανταλλαγής πληροφοριών με εξειδικευμένους παρόχους, συμπεριλαμβανομένων παρόχων διαχειριζόμενων λύσεων ασφάλειας και εταιρειών, προκειμένου να συμβάλει στην αποστολή του ENISA για την επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση. Με βάση τη συνεργασία με τα ενδιαφερόμενα μέρη, συμπεριλαμβανομένου του ιδιωτικού τομέα, η έκθεση εξέτασης συγκεκριμένων περιστατικών θα πρέπει να αποσκοπεί στην αξιολόγηση των αιτίων, των επιπτώσεων και των μέτρων μετριασμού ενός περιστατικού, μετά την επέλευση του. Ιδιαίτερη προσοχή θα πρέπει να δοθεί στις πληροφορίες και τα διδάγματα που ανταλλάσσουν οι πάροχοι διαχειριζόμενων υπηρεσιών ασφάλειας που πληρούν τις προϋποθέσεις της ύψιστης επαγγελματικής ακεραιότητας, αμεροληψίας και της απαιτούμενης τεχνικής εμπειρογνωσίας, όπως απαιτείται από τον παρόντα κανονισμό. Η έκθεση θα πρέπει να υποβάλλεται και να αξιοποιείται στο πλαίσιο των εργασιών του EU-CyCLONe, του δικτύου CSIRT και της Επιτροπής. Όταν το περιστατικό αφορά τρίτη χώρα, θα πρέπει να κοινοποιείται από την Επιτροπή στον/στην ύπατο/-η εκπρόσωπο.

(37) Λαμβάνοντας υπόψη την απρόβλεπτη φύση των κυβερνοεπιθέσεων και το γεγονός ότι συχνά δεν περιορίζονται σε συγκεκριμένη γεωγραφική περιοχή και ενέχουν υψηλό κίνδυνο δευτερογενών επιπτώσεων, η ενίσχυση της ανθεκτικότητας των γειτονικών χωρών και της ικανότητάς τους να αντιμετωπίζουν αποτελεσματικά σημαντικά και μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας συμβάλλει στην προστασία της Ένωσης στο σύνολό της. Ως εκ τούτου, οι τρίτες χώρες που είναι συνδεδεμένες με το πρόγραμμα «Ψηφιακή Ευρώπη» μπορούν να λαμβάνουν στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, εφόσον αυτό

προβλέπεται στην αντίστοιχη συμφωνία σύνδεσης με το πρόγραμμα «Ψηφιακή Ευρώπη». Η χρηματοδότηση συνδεδεμένων τρίτων χωρών θα πρέπει να στηρίζεται από την Ένωση στο πλαίσιο σχετικών εταιρικών σχέσεων και χρηματοδοτικών μέσων για τις εν λόγω χώρες. Η στήριξη θα πρέπει να καλύπτει υπηρεσίες στον τομέα της αντιμετώπισης και της άμεσης ανάκαμψης από σημαντικά ή μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας. Οι προϋποθέσεις που καθορίζονται στον παρόντα κανονισμό για την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας και για τους αξιόπιστους παρόχους θα πρέπει να εφαρμόζονται κατά την παροχή στήριξης στις τρίτες χώρες που είναι συνδεδεμένες με το πρόγραμμα «Ψηφιακή Ευρώπη».

(38) Προκειμένου να εξασφαλιστούν ενιαίες προϋποθέσεις για την εκτέλεση του παρόντος κανονισμού, θα πρέπει να ανατεθούν στην Επιτροπή εκτελεστικές αρμοδιότητες για τον προσδιορισμό των προϋποθέσεων για τη διαλειτουργικότητα μεταξύ των διασυνοριακών SOC· τον καθορισμό των διαδικαστικών ρυθμίσεων για την ανταλλαγή πληροφοριών σχετικά με δυνητικό ή εξελισσόμενο μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας μεταξύ διασυνοριακών SOC και οντοτήτων της Ένωσης· τον καθορισμό τεχνικών απαιτήσεων για τη διασφάλιση της ασφάλειας της ευρωπαϊκής κυβερνοασπίδας· τον προσδιορισμό των ειδών και του αριθμού των υπηρεσιών αντιμετώπισης που απαιτούνται για την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας· και τον περαιτέρω καθορισμό των λεπτομερών ρυθμίσεων για την κατανομή των υπηρεσιών υποστήριξης της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. Οι εν λόγω αρμοδιότητες θα πρέπει να ασκούνται σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 182/2011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

(39) Ο στόχος του παρόντος κανονισμού μπορεί να επιτευχθεί καλύτερα σε επίπεδο Ένωσης απ’ ό,τι από τα κράτη μέλη. Επομένως, η Ένωση μπορεί να θεσπίσει μέτρα σύμφωνα με την αρχή της επικουρικότητας και της αναλογικότητας που ορίζονται στο άρθρο 5 της Συνθήκης για την Ευρωπαϊκή Ένωση. Ο παρών κανονισμός δεν υπερβαίνει τα αναγκαία όρια για την επίτευξη του εν λόγω στόχου,

ΕΞΕΔΩΣΑΝ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

## *Κεφάλαιο I*

## *ΓΕΝΙΚΟΙ ΣΤΟΧΟΙ, ΑΝΤΙΚΕΙΜΕΝΟ ΚΑΙ ΟΡΙΣΜΟΙ*

### *Άρθρο 1*

### **Αντικείμενο και στόχοι**

1. Ο παρών κανονισμός θεσπίζει μέτρα για την ενίσχυση των ικανοτήτων της Ένωσης να ανιχνεύει, να προετοιμάζεται και να αντιμετωπίζει απειλές και περιστατικά κυβερνοασφάλειας, ιδίως μέσω των ακόλουθων δράσεων:

α) ανάπτυξη πανευρωπαϊκής υποδομής κέντρων επιχειρήσεων ασφάλειας (στο εξής: ευρωπαϊκή κυβερνοασπίδα) για την οικοδόμηση και ενίσχυση κοινών ικανοτήτων ανίχνευσης και αντίληψης της κατάστασης,

β) δημιουργία μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο με σκοπό τη στήριξη των κρατών μελών όσον αφορά την προετοιμασία, την αντιμετώπιση και την άμεση ανάκαμψη από σημαντικά και μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας,

γ) θέσπιση ενός ευρωπαϊκού μηχανισμού εξέτασης περιστατικών κυβερνοασφάλειας για την εξέταση και την αξιολόγηση σημαντικών ή μεγάλης κλίμακας περιστατικών.

2. Ο παρών κανονισμός επιδιώκει τον στόχο της ενίσχυσης της αλληλεγγύης σε επίπεδο Ένωσης μέσω των ακόλουθων ειδικών στόχων:

α) την ενίσχυση της κοινής ενωσιακής ανίχνευσης και αντίληψης της κατάστασης όσον αφορά απειλές και περιστατικά στον κυβερνοχώρο, ώστε να παρέχεται η δυνατότητα ενίσχυσης της ανταγωνιστικής θέσης των τομέων της βιομηχανίας και των υπηρεσιών στην Ένωση σε ολόκληρη την ψηφιακή οικονομία και συμβολής στην τεχνολογική κυριαρχία της Ένωσης στον τομέα της κυβερνοασφάλειας,

β) την αύξηση του βαθμού ετοιμότητας των οντοτήτων που δραστηριοποιούνται σε τομείς κρίσιμης και εξαιρετικά κρίσιμης σημασίας σε ολόκληρη την Ένωση και την ενίσχυση της αλληλεγγύης με την ανάπτυξη κοινών ικανοτήτων αντιμετώπισης σημαντικών ή μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας, μεταξύ άλλων με την εξασφάλιση ενωσιακής στήριξης για την αντιμετώπιση περιστατικών κυβερνοασφάλειας σε τρίτες χώρες που είναι συνδεδεμένες με το πρόγραμμα «Ψηφιακή Ευρώπη»,

γ) την ενίσχυση της ανθεκτικότητας της Ένωσης και τη συμβολή στην αποτελεσματική αντιμετώπιση με την εξέταση και την αξιολόγηση σημαντικών ή μεγάλης κλίμακας περιστατικών, συμπεριλαμβανομένης της άντλησης διδαγμάτων και, κατά περίπτωση, συστάσεων.

3. Ο παρών κανονισμός δεν θίγει την πρωταρχική ευθύνη των κρατών μελών για την εθνική ασφάλεια, τη δημόσια ασφάλεια και την πρόληψη, διερεύνηση, εντοπισμό και δίωξη ποινικών αδικημάτων.

*Άρθρο 2*

**Ορισμοί**

Για τους σκοπούς του παρόντος κανονισμού, ισχύουν οι ακόλουθοι ορισμοί:

1) **«διασυνοριακό κέντρο επιχειρήσεων ασφάλειας» (στο εξής: διασυνοριακό SOC):** πολυεθνική πλατφόρμα που συγκεντρώνει σε μια συντονισμένη δομή δικτύου τα εθνικά SOC από τουλάχιστον τρία κράτη μέλη που συγκροτούν κοινοπραξία υποδοχής, και η οποία έχει σχεδιαστεί για την πρόληψη απειλών και περιστατικών στον κυβερνοχώρο και για την υποστήριξη της παραγωγής πληροφοριών υψηλής ποιότητας, ιδίως μέσω της ανταλλαγής δεδομένων από διάφορες πηγές, δημόσιες και ιδιωτικές, καθώς και μέσω της ανταλλαγής εργαλείων αιχμής και της από κοινού

ανάπτυξης ικανοτήτων ανίχνευσης, ανάλυσης, πρόληψης και προστασίας στον κυβερνοχώρο σε ένα αξιόπιστο περιβάλλον·

2) **«δημόσιος φορέας»:** φορέας δημοσίου δικαίου, όπως ορίζεται στο άρθρο 2 παράγραφος 1 σημείο 4) της οδηγίας 2014/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[18].

3) **«κοινοπραξία υποδοχής»:** κοινοπραξία αποτελούμενη από συμμετέχοντα κράτη, εκπροσωπούμενα από εθνικά SOC, τα οποία έχουν συμφωνήσει να δημιουργήσουν και να συμβάλουν στην αγορά εργαλείων και υποδομών για ένα διασυνοριακό SOC και στη λειτουργία αυτού·

4) «**οντότητα»:** οντότητα όπως ορίζεται στο άρθρο 6 σημείο 38 της οδηγίας (ΕΕ) 2022/2555·

5) «**οντότητες που δραστηριοποιούνται σε τομείς κρίσιμης και εξαιρετικά κρίσιμης σημασίας»:** τύπος οντοτήτων που απαριθμούνται στα παραρτήματα Ι και ΙΙ της οδηγίας (ΕΕ) 2022/2555·

6) «**κυβερνοαπειλή»:** κυβερνοαπειλή όπως ορίζεται στο άρθρο 2 σημείο 8 του κανονισμού (ΕΕ) 2019/881·

7) «**σημαντικό περιστατικό κυβερνοασφάλειας»:** περιστατικό κυβερνοασφάλειας που πληροί τα κριτήρια που ορίζονται στο άρθρο 23 παράγραφος 3 της οδηγίας (ΕΕ) 2022/2555·

8) «**περιστατικό μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας»:** περιστατικό όπως ορίζεται στο άρθρο 6 σημείο 7 της οδηγίας (ΕΕ) 2022/2555·

9) **«ετοιμότητα»:** κατάσταση ετοιμότητας και ικανότητας για τη διασφάλιση αποτελεσματικής ταχείας αντίδρασης σε σημαντικό ή μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας, η οποία επιτυγχάνεται ως αποτέλεσμα των δράσεων εκτίμησης κινδύνων και παρακολούθησης που λαμβάνονται εκ των προτέρων·

10) **«αντιμετώπιση»:** δράση σε περίπτωση σημαντικού ή μεγάλης κλίμακας περιστατικού στον τομέα της κυβερνοασφάλειας, ή κατά τη διάρκεια ή μετά το περιστατικό αυτό, για την αντιμετώπιση των άμεσων και βραχυπρόθεσμων δυσμενών συνεπειών του·

11) **«αξιόπιστοι πάροχοι»:** πάροχοι διαχειριζόμενων υπηρεσιών ασφάλειας, όπως ορίζονται στο άρθρο 6 σημείο 40 της οδηγίας (ΕΕ) 2022/2555, οι οποίοι επιλέγονται σύμφωνα με το άρθρο 16 του παρόντος κανονισμού.

[18] Οδηγία 2014/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Φεβρουαρίου 2014, σχετικά με τις διαδικασίες σύναψης δημοσίων συμβάσεων και την κατάργηση της οδηγίας 2004/18/ΕΚ (ΕΕ L 94 της 28.3.2014, σ. 65).

## *Κεφάλαιο ΙΙ*

## *Η ΕΥΡΩΠΑΪΚΗ ΚΥΒΕΡΝΟΑΣΠΙΔΑ*

*Άρθρο 3*

**Θέσπιση της ευρωπαϊκής κυβερνοασπίδας**

1. Θεσπίζεται διασυνδεδεμένη πανευρωπαϊκή υποδομή κέντρων επιχειρήσεων ασφάλειας (στο εξής: ευρωπαϊκή κυβερνοασπίδα) με σκοπό την ανάπτυξη προηγμένων ικανοτήτων της Ένωσης για την ανίχνευση, την ανάλυση και την επεξεργασία δεδομένων σχετικά με απειλές και περιστατικά στον κυβερνοχώρο στην Ένωση. Η κυβερνοασπίδα αποτελείται από το σύνολο των εθνικών κέντρων επιχειρήσεων ασφάλειας (στο εξής: εθνικά SOC) και των διασυνοριακών κέντρων επιχειρήσεων ασφάλειας (στο εξής: διασυνοριακά SOC).

Οι δράσεις που υλοποιούν την ευρωπαϊκή κυβερνοασπίδα στηρίζονται από χρηματοδότηση από το πρόγραμμα «Ψηφιακή Ευρώπη» και υλοποιούνται σύμφωνα με τον κανονισμό (ΕΕ) 2021/694 και ιδίως τον ειδικό στόχο 3.

2. Η ευρωπαϊκή κυβερνοασπίδα:

α) συγκεντρώνει και επιτρέπει την ανταλλαγή δεδομένων σχετικά με απειλές και περιστατικά στον κυβερνοχώρο από διάφορες πηγές μέσω διασυνοριακών SOC,

β) παράγει υψηλής ποιότητας και αξιοποιήσιμες πληροφορίες και πληροφορίες για κυβερνοαπειλές, μέσω της χρήσης εργαλείων αιχμής, ιδίως τεχνολογιών τεχνητής νοημοσύνης και ανάλυσης δεδομένων,

γ) συμβάλλει στην καλύτερη προστασία και αντιμετώπιση των κυβερνοαπειλών,

δ) συμβάλλει στην ταχύτερη ανίχνευση των κυβερνοαπειλών και στην αντίληψη της κατάστασης σε ολόκληρη την Ένωση,

ε) παρέχει υπηρεσίες και δραστηριότητες για την κοινότητα κυβερνοασφάλειας στην Ένωση, μεταξύ άλλων συμβάλλοντας στην ανάπτυξη προηγμένων εργαλείων τεχνητής νοημοσύνης και ανάλυσης δεδομένων.

Αναπτύσσεται σε συνεργασία με την πανευρωπαϊκή υποδομή υπολογιστικής υψηλών επιδόσεων που θεσπίστηκε δυνάμει του κανονισμού (ΕΕ) 2021/1173.

*Άρθρο 4*

**Εθνικά κέντρα επιχειρήσεων ασφάλειας**

1. Για να συμμετάσχει στην ευρωπαϊκή κυβερνοασπίδα, κάθε κράτος μέλος ορίζει τουλάχιστον ένα εθνικό SOC. Το εθνικό SOC είναι δημόσιος φορέας.

Έχει την ικανότητα να λειτουργεί ως σημείο αναφοράς και πύλη προς άλλους δημόσιους και ιδιωτικούς οργανισμούς σε εθνικό επίπεδο για τη συλλογή και ανάλυση πληροφοριών

σχετικά με απειλές και περιστατικά κυβερνοασφάλειας και για τη συμβολή σε διασυνοριακό SOC. Είναι εφοδιασμένο με προηγμένες τεχνολογίες ανίχνευσης, συγκέντρωσης και ανάλυσης δεδομένων σχετικών με απειλές και περιστατικά κυβερνοασφάλειας.

2. Κατόπιν πρόσκλησης εκδήλωσης ενδιαφέροντος, τα εθνικά SOC επιλέγονται από το Ευρωπαϊκό Κέντρο Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας (στο εξής: ECCC) για να συμμετάσχουν σε κοινή διαδικασία προμήθειας εργαλείων και υποδομών με το ECCC. Το ECCC μπορεί να χορηγεί επιχορηγήσεις στα επιλεγμένα εθνικά SOC για τη χρηματοδότηση της λειτουργίας των εν λόγω εργαλείων και υποδομών. Η χρηματοδοτική συνεισφορά της Ένωσης καλύπτει έως και το 50 % του κόστους αγοράς των εργαλείων και των υποδομών και έως το 50 % του κόστους λειτουργίας, ενώ το υπόλοιπο κόστος καλύπτεται από το κράτος μέλος. Πριν από την έναρξη της διαδικασίας για την αγορά των εργαλείων και των υποδομών, το ECCC και το εθνικό SOC συνάπτουν συμφωνία υποδοχής και χρήσης που ρυθμίζει τη χρήση των εργαλείων και των υποδομών.

3. Το εθνικό SOC που επιλέγεται σύμφωνα με την παράγραφο 2 δεσμεύεται να υποβάλει αίτηση συμμετοχής σε διασυνοριακό SOC εντός δύο ετών από την ημερομηνία αγοράς των εργαλείων και των υποδομών ή από την ημερομηνία κατά την οποία λαμβάνει επιχορήγηση, όποιο από τα δύο συμβεί νωρίτερα. Εάν ένα εθνικό SOC δεν συμμετέχει μέχρι τότε σε διασυνοριακό SOC, δεν είναι επιλέξιμο για πρόσθετη στήριξη της Ένωσης δυνάμει του παρόντος κανονισμού.

*Άρθρο 5*

**Διασυνοριακά κέντρα επιχειρήσεων ασφάλειας**

1. Κοινοπραξία υποδοχής αποτελούμενη από τουλάχιστον τρία κράτη μέλη, εκπροσωπούμενα από εθνικά SOC, που δεσμεύονται να συνεργαστούν για τον συντονισμό των δραστηριοτήτων τους με σκοπό την ανίχνευση και την παρακολούθηση απειλών στον κυβερνοχώρο, είναι επιλέξιμη για συμμετοχή σε δράσεις για τη δημιουργία διασυνοριακού SOC.

2. Κατόπιν πρόσκλησης εκδήλωσης ενδιαφέροντος, η κοινοπραξία υποδοχής επιλέγεται από το ECCC για να συμμετάσχει σε κοινή διαδικασία προμήθειας εργαλείων και υποδομών με το ECCC. Το ECCC μπορεί να χορηγεί στην κοινοπραξία υποδοχής επιχορήγηση για τη χρηματοδότηση της λειτουργίας των εργαλείων και των υποδομών. Η χρηματοδοτική συνεισφορά της Ένωσης καλύπτει έως και το 75 % του κόστους αγοράς των εργαλείων και των υποδομών και έως το 50 % του κόστους λειτουργίας, ενώ το υπόλοιπο κόστος καλύπτεται από την κοινοπραξία υποδοχής. Πριν από την έναρξη της διαδικασίας αγοράς των εργαλείων και των υποδομών, το ECCC και η κοινοπραξία υποδοχής συνάπτουν συμφωνία υποδοχής και χρήσης που ρυθμίζει τη χρήση των εργαλείων και των υποδομών.

3. Τα μέλη της κοινοπραξίας υποδοχής συνάπτουν γραπτή συμφωνία κοινοπραξίας στην οποία καθορίζονται οι εσωτερικές τους ρυθμίσεις όσον αφορά την εφαρμογή της συμφωνίας υποδοχής και χρήσης.

4. Ένα διασυνοριακό SOC εκπροσωπείται για νομικούς σκοπούς από ένα εθνικό SOC που ενεργεί ως SOC συντονισμού ή από την κοινοπραξία υποδοχής, εάν αποτελεί νομικό πρόσωπο. Το SOC συντονισμού είναι υπεύθυνο για τη συμμόρφωση προς τις απαιτήσεις της συμφωνίας υποδοχής και χρήσης και του παρόντος κανονισμού.

*Άρθρο 6*

**Συνεργασία και ανταλλαγή πληροφοριών εντός και μεταξύ διασυνοριακών SOC**

1. Τα μέλη μιας κοινοπραξίας υποδοχής ανταλλάσσουν μεταξύ τους σχετικές πληροφορίες στο πλαίσιο της διασυνοριακής SOC, συμπεριλαμβανομένων πληροφοριών που αφορούν κυβερνοαπειλές, παρ' ολίγον περιστατικά, τρωτά σημεία, τεχνικές και διαδικασίες, ενδείξεις της παραβίασης, εχθρικές τακτικές, πληροφορίες που αφορούν συγκεκριμένους παράγοντες απειλής, προειδοποιήσεις για την κυβερνοασφάλεια και συστάσεις σχετικά με την παραμετροποίηση εργαλείων κυβερνοασφάλειας για τον εντοπισμό κυβερνοεπιθέσεων, στον βαθμό που η εν λόγω ανταλλαγή πληροφοριών:

α) αποσκοπεί στην πρόληψη, τον εντοπισμό, την αντιμετώπιση ή την ανάκαμψη από περιστατικά ή στον μετριασμό των επιπτώσεών τους,

β) ενισχύει το επίπεδο της κυβερνοασφάλειας, ιδίως μέσω της ευαισθητοποίησης σχετικά με τις κυβερνοαπειλές, του περιορισμού ή της παρεμπόδισης της ικανότητας διάδοσης των εν λόγω απειλών, της στήριξης μιας σειράς αμυντικών ικανοτήτων, της αποκατάστασης και της γνωστοποίησης τρωτών σημείων, της ανίχνευσης απειλών, των τεχνικών περιορισμού και πρόληψης, των στρατηγικών μετριασμού ή των σταδίων αντίδρασης και ανάκαμψης ή της προώθησης της συνεργατικής έρευνας για τις απειλές μεταξύ δημόσιων και ιδιωτικών φορέων.

2. Στην γραπτή συμφωνία κοινοπραξίας που αναφέρεται στο άρθρο 5 παράγραφος 3 καθορίζονται τα ακόλουθα:

α) δέσμευση για ανταλλαγή σημαντικού όγκου δεδομένων που αναφέρονται στην παράγραφο 1 και οι προϋποθέσεις υπό τις οποίες πρέπει να ανταλλάσσονται οι εν λόγω πληροφορίες,

β) ένα πλαίσιο διακυβέρνησης που θα παρέχει κίνητρα για την ανταλλαγή πληροφοριών από όλους τους συμμετέχοντες,

γ) στόχοι για τη συμβολή στην ανάπτυξη προηγμένων εργαλείων τεχνητής νοημοσύνης και ανάλυσης δεδομένων.

3. Για να ενθαρρυνθεί η ανταλλαγή πληροφοριών μεταξύ των διασυνοριακών SOC, τα διασυνοριακά SOC εξασφαλίζουν υψηλό επίπεδο διαλειτουργικότητας μεταξύ τους. Για τη διευκόλυνση της διαλειτουργικότητας μεταξύ των διασυνοριακών SOC, η Επιτροπή μπορεί, με εκτελεστικές πράξεις, αφού ζητήσει τη γνώμη του ECCC, να καθορίζει τους όρους της εν λόγω διαλειτουργικότητας. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 21 παράγραφος 2 του παρόντος κανονισμού.

4. Τα διασυνοριακά SOC συνάπτουν μεταξύ τους συμφωνίες συνεργασίας, στις οποίες καθορίζονται οι αρχές ανταλλαγής πληροφοριών μεταξύ των διασυνοριακών πλατφορμών.

*Άρθρο 7*

**Συνεργασία και ανταλλαγή πληροφοριών με οντότητες της Ένωσης**

1. Όταν τα διασυνοριακά SOC λαμβάνουν πληροφορίες σχετικά με δυνητικό ή εξελισσόμενο μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας, παρέχουν σχετικές

πληροφορίες στο EU-CyCLONe, στο δίκτυο CSIRT και στην Επιτροπή, λαμβανομένων υπόψη των αντίστοιχων ρόλων τους όσον αφορά τη διαχείριση κρίσεων σύμφωνα με την οδηγία (ΕΕ) 2022/2555, χωρίς αδικαιολόγητη καθυστέρηση.

2. Η Επιτροπή δύναται να καθορίζει, με εκτελεστικές πράξεις, τις διαδικαστικές ρυθμίσεις για την ανταλλαγή πληροφοριών που προβλέπεται στην παράγραφο 1. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 21 παράγραφος 2 του παρόντος κανονισμού.

*Άρθρο 8*

**Ασφάλεια**

1. Τα κράτη μέλη που συμμετέχουν στην ευρωπαϊκή κυβερνοασπίδα διασφαλίζουν υψηλό επίπεδο ασφάλειας των δεδομένων και υλικής ασφάλειας της υποδομής της ευρωπαϊκής κυβερνοασπίδας και μεριμνούν για την κατάλληλη διαχείριση και έλεγχο της υποδομής ώστε να προστατεύεται από απειλές και να διασφαλίζεται η ασφάλειά της και η ασφάλεια των συστημάτων, συμπεριλαμβανομένης της ασφάλειας των δεδομένων που ανταλλάσσονται μέσω της υποδομής.

2. Τα κράτη μέλη που συμμετέχουν στην ευρωπαϊκή κυβερνοασπίδα διασφαλίζουν ότι η ανταλλαγή πληροφοριών στο πλαίσιο της ευρωπαϊκής κυβερνοασπίδας με οντότητες που δεν είναι δημόσιοι φορείς των κρατών μελών δεν επηρεάζει αρνητικά τα συμφέροντα ασφάλειας της Ένωσης.

3. Η Επιτροπή δύναται να εκδίδει εκτελεστικές πράξεις για τον καθορισμό τεχνικών απαιτήσεων ώστε τα κράτη μέλη να συμμορφώνονται προς την υποχρέωση που υπέχουν δυνάμει των παραγράφων 1 και 2. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 21 παράγραφος 2 του παρόντος κανονισμού. Στο πλαίσιο αυτό, η Επιτροπή, υποστηριζόμενη από τον/την ύπατο/-η εκπρόσωπο, λαμβάνει υπόψη τα σχετικά πρότυπα ασφάλειας σε επίπεδο άμυνας, προκειμένου να διευκολύνει τη συνεργασία με στρατιωτικούς φορείς.

## *Κεφάλαιο III*

## *ΜΗΧΑΝΙΣΜΟΣ ΕΚΤΑΚΤΗΣ ΑΝΑΓΚΗΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ*

*Άρθρο 9*

**Θέσπιση του μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο**

1. Θεσπίζεται μηχανισμός έκτακτης ανάγκης στον κυβερνοχώρο με σκοπό τη βελτίωση της ανθεκτικότητας της Ένωσης σε μείζονες απειλές κυβερνοασφάλειας και την προετοιμασία και τον μετριασμό, σε πνεύμα αλληλεγγύης, των βραχυπρόθεσμων επιπτώσεων σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας (στο εξής: μηχανισμός).

2. Οι δράσεις που υλοποιούν τον μηχανισμό έκτακτης ανάγκης στον κυβερνοχώρο στηρίζονται από χρηματοδότηση από το πρόγραμμα «Ψηφιακή Ευρώπη» και υλοποιούνται σύμφωνα με τον κανονισμό (ΕΕ) 2021/694 και ιδίως τον ειδικό στόχο 3.

*Άρθρο 10*

**Είδος δράσεων**

1. Ο μηχανισμός παρέχει τα ακόλουθα είδη δράσεων:

α) δράσεις ετοιμότητας, συμπεριλαμβανομένων των συντονισμένων δοκιμών ετοιμότητας οντοτήτων που δραστηριοποιούνται σε τομείς εξαιρετικά κρίσιμης σημασίας σε ολόκληρη την Ένωση,

β) δράσεις αντιμετώπισης, οι οποίες στηρίζουν την αντιμετώπιση σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας και την άμεση ανάκαμψη από αυτά, και οι οποίες πρέπει να παρέχονται από αξιόπιστους παρόχους που συμμετέχουν στην εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας που θεσπίζεται δυνάμει του άρθρου 12,

γ) δράσεις αμοιβαίας συνδρομής που συνίστανται στην παροχή συνδρομής από τις εθνικές αρχές ενός κράτους μέλους σε άλλο κράτος μέλος, ιδίως όπως προβλέπεται στο άρθρο 11 παράγραφος 3 στοιχείο στ) της οδηγίας (ΕΕ) 2022/2555.

*Άρθρο 11*

**Συντονισμένες δοκιμές ετοιμότητας οντοτήτων**

1. Για τους σκοπούς της στήριξης των συντονισμένων δοκιμών ετοιμότητας των οντοτήτων που αναφέρονται στο άρθρο 10 παράγραφος 1 στοιχείο α), σε ολόκληρη την Ένωση, η Επιτροπή, αφού ζητήσει τη γνώμη της ομάδας συνεργασίας NIS και του ENISA, προσδιορίζει τους σχετικούς τομείς, ή υποτομείς, από τους τομείς υψηλής κρισιμότητας που παρατίθενται στο παράρτημα Ι της οδηγίας (ΕΕ) 2022/2555, των οποίων οι οντότητες μπορούν να υποβληθούν σε συντονισμένες δοκιμές ετοιμότητας, λαμβάνοντας υπόψη τις υφιστάμενες και προγραμματισμένες συντονισμένες εκτιμήσεις κινδύνου και δοκιμές ανθεκτικότητας σε επίπεδο Ένωσης.

2. Η ομάδα συνεργασίας NIS, σε συνεργασία με την Επιτροπή, τον ENISA και τον/την ύπατο/-η εκπρόσωπο, αναπτύσσει κοινά σενάρια και μεθοδολογίες κινδύνου για τις συντονισμένες δοκιμές.

*Άρθρο 12*

**Σύσταση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας**

1. Δημιουργείται εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, με σκοπό να βοηθήσει τους χρήστες που αναφέρονται στην παράγραφο 3 να αντιμετωπίζουν ή να παρέχουν στήριξη για την αντιμετώπιση σημαντικών ή μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας και την άμεση ανάκαμψη από τέτοια περιστατικά.

2. Η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας συνίσταται σε υπηρεσίες αντιμετώπισης περιστατικών από αξιόπιστους παρόχους που επιλέγονται σύμφωνα με τα κριτήρια που ορίζονται στο άρθρο 16. Η εφεδρεία περιλαμβάνει προδεσμευμένες υπηρεσίες. Οι υπηρεσίες μπορούν να αναπτυχθούν σε όλα τα κράτη μέλη.

3. Οι χρήστες των υπηρεσιών από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας περιλαμβάνουν:

α) αρχές διαχείρισης κυβερνοκρίσεων των κρατών μελών και CSIRT, όπως αναφέρονται στο άρθρο 9 παράγραφοι 1 και 2 και στο άρθρο 10 της οδηγίας (ΕΕ) 2022/2555, αντίστοιχα,

β) τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης.

4. Οι χρήστες που αναφέρονται στην παράγραφο 3 στοιχείο α) χρησιμοποιούν τις υπηρεσίες της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας για την αντιμετώπιση ή την υποστήριξη της αντιμετώπισης και της άμεσης ανάκαμψης από σημαντικά ή μεγάλης κλίμακας περιστατικά που επηρεάζουν οντότητες που δραστηριοποιούνται σε τομείς κρίσιμης ή εξαιρετικά κρίσιμης σημασίας.

5. Η Επιτροπή έχει τη συνολική ευθύνη για την υλοποίηση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. Η Επιτροπή καθορίζει τις προτεραιότητες και την εξέλιξη της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, σύμφωνα με τις απαιτήσεις των χρηστών που αναφέρονται στην παράγραφο 3, εποπτεύει την υλοποίησή της και διασφαλίζει τη συμπληρωματικότητα, τη συνοχή, τις συνέργειες και τους δεσμούς με άλλες δράσεις στήριξης στο πλαίσιο του παρόντος κανονισμού, καθώς και με άλλες δράσεις και προγράμματα της Ένωσης.

6. Η Επιτροπή μπορεί να αναθέσει τη λειτουργία και τη διαχείριση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, εν όλω ή εν μέρει, στον ENISA, μέσω συμφωνιών συνεισφοράς.

7. Προκειμένου να στηρίξει την Επιτροπή στη δημιουργία της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, ο ENISA εκπονεί χαρτογράφηση των αναγκαίων υπηρεσιών, αφού ζητήσει τη γνώμη των κρατών μελών και της Επιτροπής. Ο ENISA εκπονεί παρόμοια χαρτογράφηση, αφού ζητήσει τη γνώμη της Επιτροπής, για τον προσδιορισμό των αναγκών των τρίτων χωρών που είναι επιλέξιμες για στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας σύμφωνα με το άρθρο 17. Η Επιτροπή, κατά περίπτωση, ζητά τη γνώμη του/της ύπατου/-ης εκπροσώπου.

8. Η Επιτροπή μπορεί, με εκτελεστικές πράξεις, να προσδιορίζει τα είδη και τον αριθμό των υπηρεσιών αντιμετώπισης που απαιτούνται για την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 21 παράγραφος 2.

*Άρθρο 13*

**Αιτήματα στήριξης από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας**

1. Οι χρήστες που αναφέρονται στο άρθρο 12 παράγραφος 3 μπορούν να ζητούν υπηρεσίες από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας για την υποστήριξη της αντιμετώπισης και της άμεσης ανάκαμψης από σημαντικά ή μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας.

2. Για να λάβουν στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, οι χρήστες που αναφέρονται στο άρθρο 12 παράγραφος 3 λαμβάνουν μέτρα για τον μετριασμό των επιπτώσεων του περιστατικού για το οποίο ζητείται η στήριξη, συμπεριλαμβανομένης της παροχής άμεσης τεχνικής βοήθειας, και άλλων πόρων για να βοηθήσουν στην αντιμετώπιση του περιστατικού, καθώς και προσπαθειών άμεσης ανάκαμψης.

3. Τα αιτήματα στήριξης από χρήστες που αναφέρονται στο άρθρο 12 παράγραφος 3 στοιχείο α) του παρόντος κανονισμού διαβιβάζονται στην Επιτροπή και στον ENISA μέσω του ενιαίου σημείου επαφής που ορίζεται ή θεσπίζεται από το κράτος μέλος σύμφωνα με το άρθρο 8 παράγραφος 3 της οδηγίας (ΕΕ) 2022/2555.

4. Τα κράτη μέλη ενημερώνουν το δίκτυο CSIRT και, κατά περίπτωση, το EU-CyCLONe σχετικά με τα αιτήματά τους για στήριξη της αντιμετώπισης περιστατικών και της άμεσης ανάκαμψης από αυτά σύμφωνα με το παρόν άρθρο.

5. Τα αιτήματα για στήριξη της αντιμετώπισης περιστατικών και της άμεσης ανάκαμψης από αυτά περιλαμβάνουν:

α) κατάλληλες πληροφορίες σχετικά με την πληγείσα οντότητα και τις πιθανές επιπτώσεις του περιστατικού και την προγραμματισμένη χρήση της αιτούμενης στήριξης, συμπεριλαμβανομένης αναφοράς των εκτιμώμενων αναγκών,

β) πληροφορίες σχετικά με τα μέτρα που λαμβάνονται για τον μετριασμό του περιστατικού για το οποίο ζητείται η στήριξη, όπως αναφέρεται στην παράγραφο 2,

γ) πληροφορίες σχετικά με άλλες μορφές στήριξης που έχει στη διάθεσή της η πληγείσα οντότητα, συμπεριλαμβανομένων των συμβατικών ρυθμίσεων που ισχύουν για τις υπηρεσίες αντιμετώπισης περιστατικών και άμεσης ανάκαμψης, καθώς και ασφαλιστήριων συμβολαίων που ενδέχεται να καλύπτουν τέτοιου είδους περιστατικά.

6. Ο ENISA, σε συνεργασία με την Επιτροπή και την ομάδα συνεργασίας NIS, καταρτίζει υπόδειγμα για τη διευκόλυνση της υποβολής αιτημάτων στήριξης από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας.

7. Η Επιτροπή μπορεί, με εκτελεστικές πράξεις, να προσδιορίζει περαιτέρω τις λεπτομερείς ρυθμίσεις για την κατανομή των υπηρεσιών στήριξης της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 21 παράγραφος 2.

*Άρθρο 14*

**Υλοποίηση της στήριξης από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας**

1. Τα αιτήματα στήριξης από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας αξιολογούνται από την Επιτροπή, με την υποστήριξη του ENISA ή όπως ορίζεται στις συμφωνίες συνεισφοράς δυνάμει του άρθρου 12 παράγραφος 6, και η απάντηση διαβιβάζεται στους χρήστες που αναφέρονται στο άρθρο 12 παράγραφος 3 χωρίς καθυστέρηση.

2. Για την ιεράρχηση των αιτημάτων, σε περίπτωση πολλαπλών παράλληλων αιτημάτων, λαμβάνονται υπόψη, κατά περίπτωση, τα ακόλουθα κριτήρια:

α) η σοβαρότητα του περιστατικού κυβερνοασφάλειας,

β) ο τύπος της πληγείσας οντότητας, με υψηλότερη προτεραιότητα σε περιστατικά που επηρεάζουν βασικές οντότητες, όπως ορίζονται στο άρθρο 3 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555,

γ) οι δυνητικές επιπτώσεις στο/-α επηρεαζόμενο/-α κράτος/-η μέλος/-η ή στους χρήστες,

δ) ο δυνητικός διασυνοριακός χαρακτήρας του περιστατικού και ο κίνδυνος πρόκλησης δευτερογενών επιπτώσεων σε άλλα κράτη μέλη ή χρήστες,

ε) τα μέτρα που λαμβάνονται από τον χρήστη για την υποβοήθηση της αντιμετώπισης και οι προσπάθειες άμεσης ανάκαμψης, όπως αναφέρονται στο άρθρο 13 παράγραφος 2 και στο άρθρο 13 παράγραφος 5 στοιχείο β).

3. Οι υπηρεσίες εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας παρέχονται σύμφωνα με ειδικές συμφωνίες μεταξύ του παρόχου υπηρεσιών και του χρήστη στον οποίο παρέχεται η στήριξη στο πλαίσιο της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. Οι εν λόγω συμφωνίες περιλαμβάνουν όρους ευθύνης.

4. Οι συμφωνίες που αναφέρονται στην παράγραφο 3 μπορούν να βασίζονται σε υποδείγματα που καταρτίζει ο ENISA, αφού ζητήσει τη γνώμη των κρατών μελών.

5. Η Επιτροπή και ο ENISA δεν φέρουν συμβατική ευθύνη για ζημίες που προκαλούνται σε τρίτους από τις υπηρεσίες που παρέχονται στο πλαίσιο της υλοποίησης της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας.

6. Εντός ενός μηνός από το τέλος της δράσης στήριξης, οι χρήστες υποβάλλουν στην Επιτροπή και στον ENISA συνοπτική έκθεση σχετικά με την παρασχεθείσα υπηρεσία, τα αποτελέσματα που επιτεύχθηκαν και τα διδάγματα που αντλήθηκαν. Όταν ο χρήστης προέρχεται από τρίτη χώρα, όπως ορίζεται στο άρθρο 17, η εν λόγω έκθεση κοινοποιείται στον/στην ύπατο/-η εκπρόσωπο.

7. Η Επιτροπή υποβάλλει τακτικά έκθεση στην ομάδα συνεργασίας NIS σχετικά με τη χρήση και τα αποτελέσματα της στήριξης.

*Άρθρο 15*

**Συντονισμός με τους μηχανισμούς διαχείρισης κρίσεων**

1. Σε περιπτώσεις όπου σημαντικά ή μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας προέρχονται από ή έχουν ως αποτέλεσμα καταστροφές, όπως ορίζονται στην απόφαση 1313/2013/ΕΕ[19], η στήριξη βάσει του παρόντος κανονισμού για την αντιμετώπιση τέτοιων περιστατικών συμπληρώνει τις δράσεις δυνάμει και με την επιφύλαξη της απόφασης 1313/2013/ΕΕ.

2. Σε περίπτωση μεγάλης κλίμακας διασυνοριακού περιστατικού στον τομέα της κυβερνοασφάλειας, όπου ενεργοποιούνται ρυθμίσεις ολοκληρωμένης αντιμετώπισης πολιτικών κρίσεων (IPCR), η στήριξη βάσει του παρόντος κανονισμού για την αντιμετώπιση

[19] Απόφαση αριθ. 1313/2013/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Δεκεμβρίου 2013, περί μηχανισμού πολιτικής προστασίας της Ένωσης (ΕΕ L 347 της 20.12.2013, σ. 924).

του εν λόγω περιστατικού αντιμετωπίζεται σύμφωνα με τα σχετικά πρωτόκολλα και διαδικασίες στο πλαίσιο των IPCR.

3. Σε διαβούλευση με τον/την ύπατο/-η εκπρόσωπο, η στήριξη στο πλαίσιο του μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο μπορεί να συμπληρώνει τη βοήθεια που παρέχεται στο πλαίσιο της κοινής εξωτερικής πολιτικής και πολιτικής ασφαλείας και της κοινής πολιτικής ασφάλειας και άμυνας, μεταξύ άλλων μέσω των ομάδων ταχείας αντίδρασης στον κυβερνοχώρο. Μπορεί επίσης να συμπληρώνει ή να συμβάλλει στη συνδρομή που παρέχεται από ένα κράτος μέλος σε άλλο κράτος μέλος στο πλαίσιο του άρθρου 42 παράγραφος 7 της Συνθήκης για την Ευρωπαϊκή Ένωση.

4. Η στήριξη στο πλαίσιο του μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο μπορεί να αποτελεί μέρος της κοινής αντίδρασης της Ένωσης και των κρατών μελών σε καταστάσεις που αναφέρονται στο άρθρο 222 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης.

*Άρθρο 16*

**Αξιόπιστοι πάροχοι**

1. Στις διαδικασίες προμηθειών με σκοπό τη δημιουργία της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, η αναθέτουσα αρχή ενεργεί σύμφωνα με τις αρχές που καθορίζονται στον κανονισμό (ΕΕ, Ευρατόμ) 2018/1046 και σύμφωνα με τις ακόλουθες αρχές:

α) διασφαλίζει ότι η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας περιλαμβάνει υπηρεσίες που μπορούν να αναπτυχθούν σε όλα τα κράτη μέλη, λαμβάνοντας ιδίως υπόψη τις εθνικές απαιτήσεις για την παροχή των εν λόγω υπηρεσιών, συμπεριλαμβανομένης της πιστοποίησης ή της διαπίστευσης,

β) διασφαλίζει την προστασία των ουσιωδών συμφερόντων ασφάλειας της Ένωσης και των κρατών μελών της,

γ) διασφαλίζει ότι η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας προσδίδει ενωσιακή προστιθέμενη αξία, συμβάλλοντας στην επίτευξη των στόχων που ορίζονται στο άρθρο 3 του κανονισμού (ΕΕ) 2021/694, συμπεριλαμβανομένης της προώθησης της ανάπτυξης δεξιοτήτων κυβερνοασφάλειας στην ΕΕ.

2. Κατά την προμήθεια υπηρεσιών για την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, η αναθέτουσα αρχή περιλαμβάνει στα έγγραφα της προμήθειας τα ακόλουθα κριτήρια επιλογής:

α) ο πάροχος αποδεικνύει ότι το προσωπικό του διαθέτει τον υψηλότερο βαθμό επαγγελματικής ακεραιότητας, ανεξαρτησίας, ευθύνης και την απαιτούμενη τεχνική επάρκεια για την εκτέλεση των δραστηριοτήτων στον συγκεκριμένο τομέα, και διασφαλίζει τη μονιμότητα/συνέχεια της εμπειρογνωσίας, καθώς και τους απαιτούμενους τεχνικούς πόρους,

β) ο πάροχος, οι θυγατρικές και οι υπεργολάβοι του εφαρμόζουν πλαίσιο για την προστασία των ευαίσθητων πληροφοριών που σχετίζονται με την υπηρεσία, και ιδίως των αποδεικτικών στοιχείων, των πορισμάτων και των εκθέσεων, και συμμορφώνεται με τους κανόνες ασφαλείας της Ένωσης για την προστασία των διαβαθμισμένων πληροφοριών της ΕΕ,

γ) ο πάροχος παρέχει επαρκείς αποδείξεις ότι η διοικητική δομή του είναι διαφανής, δεν είναι πιθανό να θέσει σε κίνδυνο την αμεροληψία του και την ποιότητα των υπηρεσιών του ή να προκαλέσει συγκρούσεις συμφερόντων,

δ) ο πάροχος διαθέτει κατάλληλη εξουσιοδότηση ασφαλείας, τουλάχιστον για το προσωπικό που προορίζεται για την ανάπτυξη υπηρεσιών,

ε) ο πάροχος διαθέτει το σχετικό επίπεδο ασφάλειας για τα συστήματα ΤΠ του,

στ) ο πάροχος είναι εξοπλισμένος με τον τεχνικό εξοπλισμό υλισμικού και λογισμικού που απαιτείται για την υποστήριξη της αιτούμενης υπηρεσίας,

ζ) ο πάροχος είναι σε θέση να αποδείξει ότι διαθέτει πείρα στην παροχή παρόμοιων υπηρεσιών σε σχετικές εθνικές αρχές ή οντότητες που δραστηριοποιούνται σε τομείς κρίσιμης ή εξαιρετικά κρίσιμης σημασίας,

η) ο πάροχος είναι σε θέση να παρέχει την υπηρεσία εντός σύντομου χρονικού διαστήματος στο κράτος μέλος/-η όπου μπορεί να παρέχει την υπηρεσία,

θ) ο πάροχος είναι σε θέση να παρέχει την υπηρεσία στην τοπική γλώσσα του κράτους μέλους ή των κρατών μελών όπου μπορεί να παρέχει την υπηρεσία,

ι) μόλις τεθεί σε εφαρμογή σύστημα πιστοποίησης της ΕΕ για τις διαχειριζόμενες υπηρεσίες ασφάλειας του κανονισμού (ΕΕ) 2019/881, ο πάροχος πιστοποιείται σύμφωνα με το εν λόγω σύστημα.

*Άρθρο 17*

**Στήριξη σε τρίτες χώρες**

1. Τρίτες χώρες μπορούν να ζητήσουν στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, εφόσον αυτό προβλέπεται από συμφωνίες σύνδεσης που έχουν συναφθεί σχετικά με τη συμμετοχή τους στο πρόγραμμα «Ψηφιακή Ευρώπη».

2. Η στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας είναι σύμφωνη προς τις διατάξεις του παρόντος κανονισμού και συμμορφώνεται με τυχόν ειδικούς όρους που καθορίζονται στις συμφωνίες σύνδεσης που αναφέρονται στην παράγραφο 1.

3. Στους χρήστες από συνδεδεμένες τρίτες χώρες που είναι επιλέξιμοι να λαμβάνουν υπηρεσίες από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας περιλαμβάνονται αρμόδιες αρχές, όπως οι CSIRT και οι αρχές διαχείρισης κυβερνοκρίσεων.

4. Κάθε τρίτη χώρα που είναι επιλέξιμη για στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας ορίζει μια αρχή που ενεργεί ως ενιαίο σημείο επαφής για τους σκοπούς του παρόντος κανονισμού.

5. Πριν λάβουν στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, οι τρίτες χώρες παρέχουν στην Επιτροπή και στον/στην ύπατο/-η εκπρόσωπο πληροφορίες σχετικά με τις ικανότητές τους όσον αφορά την κυβερνοανθεκτικότητα και τη διαχείριση κινδύνων, συμπεριλαμβανομένων τουλάχιστον πληροφοριών σχετικά με τα εθνικά μέτρα που λαμβάνονται για την προετοιμασία για σημαντικά ή μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας, καθώς και πληροφοριών σχετικά με τις αρμόδιες εθνικές οντότητες, συμπεριλαμβανομένων των CSIRT ή ανάλογων οντοτήτων, τις ικανότητές τους και τους πόρους που τους διατίθενται. Όταν οι διατάξεις των άρθρων 13 και 14 του παρόντος κανονισμού αναφέρονται σε κράτη μέλη, εφαρμόζονται σε τρίτες χώρες όπως ορίζεται στην παράγραφο 1.

6. Η Επιτροπή συντονίζει με τον/την ύπατο/-η εκπρόσωπο τα αιτήματα που λαμβάνει και την υλοποίηση της στήριξης που παρέχεται σε τρίτες χώρες από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας.

## *Κεφάλαιο IV*

## *ΜΗΧΑΝΙΣΜΟΣ ΕΞΕΤΑΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ*

### *Άρθρο 18*

### **Μηχανισμός εξέτασης περιστατικών κυβερνοασφάλειας**

1. Κατόπιν αιτήματος της Επιτροπής, του EU-CyCLONe ή του δικτύου CSIRT, ο ENISA θα πρέπει να εξετάζει και να αξιολογεί απειλές, τρωτά σημεία και δράσεις μετριασμού σε σχέση με συγκεκριμένο σημαντικό ή μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας. Μετά την ολοκλήρωση της εξέτασης και της αξιολόγησης ενός περιστατικού, ο ENISA υποβάλλει έκθεση εξέτασης περιστατικού στο δίκτυο CSIRT, στο EU-CyCLONe και στην Επιτροπή για να τους στηρίξει κατά την εκτέλεση των καθηκόντων τους, ιδίως όσον αφορά τα καθήκοντα που ορίζονται στα άρθρα 15 και 16 της οδηγίας (ΕΕ) 2022/2555. Κατά περίπτωση, η Επιτροπή κοινοποιεί την έκθεση στον/στην ύπατο/-η εκπρόσωπο.

2. Για την εκπόνηση της έκθεσης εξέτασης περιστατικού που αναφέρεται στην παράγραφο 1, ο ENISA συνεργάζεται με όλα τα σχετικά ενδιαφερόμενα μέρη, συμπεριλαμβανομένων εκπροσώπων των κρατών μελών, της Επιτροπής, άλλων σχετικών θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ, παρόχων διαχειριζόμενων υπηρεσιών ασφάλειας και χρηστών υπηρεσιών κυβερνοασφάλειας. Κατά περίπτωση, ο ENISA συνεργάζεται επίσης με οντότητες που πλήττονται από σημαντικά ή μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας. Για την υποστήριξη της εξέτασης, ο ENISA μπορεί επίσης να συμβουλεύεται άλλα είδη ενδιαφερόμενων μερών. Οι εκπρόσωποι των οποίων ζητείται η γνώμη γνωστοποιούν κάθε πιθανή σύγκρουση συμφερόντων.

3. Η έκθεση καλύπτει εξέταση και ανάλυση του συγκεκριμένου σημαντικού ή μεγάλης κλίμακας περιστατικού στον τομέα της κυβερνοασφάλειας, συμπεριλαμβανομένων των κύριων αιτίων, των τρωτών σημείων και των διδαγμάτων που αντλήθηκαν. Προστατεύει τις εμπιστευτικές πληροφορίες, σύμφωνα με το ενωσιακό ή το εθνικό δίκαιο σχετικά με την προστασία ευαίσθητων ή διαβαθμισμένων πληροφοριών.

4. Κατά περίπτωση, η έκθεση διατυπώνει συστάσεις για τη βελτίωση της στάσης της Ένωσης στον κυβερνοχώρο.

5. Όπου είναι δυνατόν, μια έκδοση της έκθεσης δημοσιοποιείται. Η έκδοση αυτή περιλαμβάνει μόνο πληροφορίες που προορίζονται για το κοινό.

## *Κεφάλαιο V*

## *ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ*

### *Άρθρο 19*

### **Τροποποιήσεις του κανονισμού (ΕΕ) 2021/694**

Ο κανονισμός (ΕΕ) 2021/694 τροποποιείται ως εξής:

1) το άρθρο 6 τροποποιείται ως εξής:

α) η παράγραφος 1 τροποποιείται ως εξής:

1) προστίθεται το ακόλουθο στοιχείο αα):

«αα) στήριξη της ανάπτυξης ενωσιακής κυβερνοασπίδας, συμπεριλαμβανομένης της ανάπτυξης, της εγκατάστασης και της λειτουργίας εθνικών και διασυνοριακών πλατφορμών SOC που συμβάλλουν στην αντίληψη της κατάστασης στην Ένωση και στην ενίσχυση των ικανοτήτων της Ένωσης όσον αφορά τη συλλογή πληροφοριών για τις κυβερνοαπειλές»·

2) προστίθεται το ακόλουθο στοιχείο ζ):

«ζ) σύσταση και λειτουργία μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο για τη στήριξη των κρατών μελών κατά την προετοιμασία και την αντιμετώπιση σημαντικών περιστατικών στον τομέα της κυβερνοασφάλειας, συμπληρωματικά προς τους εθνικούς πόρους και ικανότητες και άλλες μορφές στήριξης που διατίθενται σε επίπεδο Ένωσης, συμπεριλαμβανομένης της δημιουργίας εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας.»·

α) η παράγραφος 2 αντικαθίσταται από το ακόλουθο κείμενο:

«2. Οι δράσεις στο πλαίσιο του ειδικού στόχου 3 εκτελούνται πρωτίστως μέσω του ευρωπαϊκού βιομηχανικού, τεχνολογικού και ερευνητικού κέντρου ικανοτήτων στον τομέα της κυβερνοασφάλειας και του δικτύου εθνικών κέντρων συντονισμού σύμφωνα με τον κανονισμό (ΕΕ) 2021/887 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[20], με εξαίρεση τις δράσεις για την υλοποίηση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, η οποία υλοποιείται από την Επιτροπή και τον ENISA.»·

2) το άρθρο 9 τροποποιείται ως εξής:

α) στην παράγραφο 2, τα στοιχεία β), γ) και δ) αντικαθίστανται από το ακόλουθο κείμενο:

«β) 1 776 956 000 EUR για τον ειδικό στόχο 2 — "Τεχνητή νοημοσύνη",

γ) 1 629 566 000 EUR για τον ειδικό στόχο 3 — "Κυβερνοασφάλεια και εμπιστοσύνη",

[20] Κανονισμός (ΕΕ) 2021/887 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Μαΐου 2021, για τη σύσταση του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας και του δικτύου εθνικών κέντρων συντονισμού (ΕΕ L 202 της 8.6.2021, σ. 1).

δ) 482 347 000 EUR για τον ειδικό στόχο 4 — “Προηγμένες ψηφιακές δεξιότητες”,»·

β) προστίθεται η ακόλουθη παράγραφος 8:

«8. Κατά παρέκκλιση από το άρθρο 12 παράγραφος 4 του κανονισμού (ΕΕ, Ευρατόμ) 2018/1046, οι μη χρησιμοποιηθείσες πιστώσεις ανάληψης υποχρεώσεων και πληρωμών για δράσεις που επιδιώκουν τους στόχους που ορίζονται στο άρθρο 6 παράγραφος 1 στοιχείο ζ) του παρόντος κανονισμού μεταφέρονται αυτομάτως και μπορούν να δεσμευθούν και να καταβληθούν έως τις 31 Δεκεμβρίου του επόμενου οικονομικού έτους.»·

3) στο άρθρο 14, η παράγραφος 2 αντικαθίσταται από το ακόλουθο κείμενο:

«2. Το πρόγραμμα μπορεί να παρέχει χρηματοδότηση με οποιαδήποτε από τις μορφές που καθορίζονται στον δημοσιονομικό κανονισμό, συμπεριλαμβανομένων κυρίως μέσω των δημοσίων συμβάσεων ως πρωταρχικής μορφής ή των επιχορηγήσεων και των βραβείων.

Αν η επίτευξη του στόχου μίας δράσης απαιτεί την προμήθεια καινοτόμων αγαθών και υπηρεσιών, οι επιχορηγήσεις μπορούν να παρασχεθούν μόνο σε δικαιούχους που είναι αναθέτουσες αρχές ή αναθέτοντες φορείς όπως ορίζονται στις οδηγίες 2014/24/EU [27] και 2014/25/EU [28] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

Αν για την επίτευξη των στόχων μίας δράσης είναι αναγκαία η προμήθεια καινοτόμων αγαθών ή υπηρεσιών που δεν είναι ακόμη διαθέσιμα στο εμπόριο σε μεγάλη κλίμακα, η αναθέτουσα αρχή ή ο αναθέτων φορέας μπορεί να επιτρέπει την ανάθεση πολλαπλών συμβάσεων στο πλαίσιο της ίδιας διαδικασίας προμήθειας.

Για δεόντως αιτιολογημένους λόγους δημόσιας ασφάλειας, η αναθέτουσα αρχή ή ο αναθέτων φορέας μπορεί να απαιτεί ο τόπος εκτέλεσης της σύμβασης να βρίσκεται εντός της επικράτειας της Ένωσης.

Κατά την εφαρμογή των διαδικασιών σύναψης συμβάσεων για την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας που θεσπίζεται με το άρθρο 12 του κανονισμού (ΕΕ) 2023/XX, η Επιτροπή και ο ENISA μπορούν να ενεργούν ως κεντρική αρχή προμηθειών για την προμήθεια εξ ονόματος τρίτων χωρών συνδεδεμένων με το πρόγραμμα σύμφωνα με το άρθρο 10. Η Επιτροπή και ο ENISA μπορούν επίσης να ενεργούν ως χονδρέμποροι, αγοράζοντας, αποθηκεύοντας και μεταπωλώντας ή δωρίζοντας προμήθειες και υπηρεσίες, συμπεριλαμβανομένων των ενοικίων, στις εν λόγω τρίτες χώρες. Κατά παρέκκλιση από το άρθρο 169 παράγραφος 3 του κανονισμού (ΕΕ). XXX/XXXX [αναδιατύπωση FR], το αίτημα μιας μόνο τρίτης χώρας αρκεί για να δοθεί εντολή στην Επιτροπή ή στον ENISA να αναλάβει δράση.

Κατά την εφαρμογή των διαδικασιών προμήθειας για την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας που θεσπίζεται με το άρθρο 12 του κανονισμού (ΕΕ) 2023/XX, η Επιτροπή και ο ENISA μπορούν να ενεργούν ως κεντρική αρχή προμηθειών για την προμήθεια εξ ονόματος των θεσμικών και λοιπών οργάνων και

οργανισμών της Ένωσης. Η Επιτροπή και ο ENISA μπορούν επίσης να ενεργούν ως χονδρέμποροι, αγοράζοντας, αποθηκεύοντας και μεταπωλώντας ή δωρίζοντας προμήθειες και υπηρεσίες, συμπεριλαμβανομένων των ενοικίων, στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης. Κατά παρέκκλιση από το άρθρο 169 παράγραφος 3 του κανονισμού (ΕΕ) XXX/XXXX [αναδιατύπωση FR], το αίτημα από ένα μόνο θεσμικό ή άλλο όργανο ή οργανισμό της Ένωσης αρκεί για να δοθεί εντολή στην Επιτροπή ή στον ENISA να αναλάβει δράση.

Το πρόγραμμα μπορεί επίσης να παρέχει χρηματοδότηση με τη μορφή χρηματοδοτικών στο πλαίσιο συνδυαστικών πράξεων.»·

4) προστίθεται το ακόλουθο άρθρο 16α:

«Στην περίπτωση δράσεων που υλοποιούν την ευρωπαϊκή κυβερνοασπίδα που θεσπίζεται με το άρθρο 3 του κανονισμού (ΕΕ) 2023/XX, οι εφαρμοστέοι κανόνες είναι εκείνοι που ορίζονται στα άρθρα 4 και 5 του κανονισμού (ΕΕ) 2023/XX. Σε περίπτωση σύγκρουσης των διατάξεων του παρόντος κανονισμού με τις διατάξεις των άρθρων 4 και 5 του κανονισμού (ΕΕ) 2023/XX, οι τελευταίες υπερισχύουν και εφαρμόζονται επί των εν λόγω συγκεκριμένων δράσεων.»·

5) το άρθρο 19 αντικαθίσταται από το ακόλουθο κείμενο:

«Η ανάθεση και η διαχείριση επιχορηγήσεων στο πλαίσιο του προγράμματος πραγματοποιούνται σύμφωνα με τον τίτλο VIII του δημοσιονομικού κανονισμού και οι επιχορηγήσεις μπορούν να καλύπτουν έως το 100 % των επιλέξιμων δαπανών, με την επιφύλαξη της αρχής της συγχρηματοδότησης που ορίζεται στο άρθρο 190 του δημοσιονομικού κανονισμού. Η ανάθεση και διαχείριση των επιχορηγήσεων αυτών γίνεται όπως καθορίζεται για κάθε ειδικό στόχο.

Στήριξη με τη μορφή επιχορηγήσεων μπορεί να χορηγείται απευθείας από το ECCC χωρίς πρόσκληση υποβολής προτάσεων προς τα εθνικά SOC που αναφέρονται στο άρθρο 4 του κανονισμού XXXX και την κοινοπραξία υποδοχής που αναφέρεται στο άρθρο 5 του κανονισμού XXXX, σύμφωνα με το άρθρο 195 παράγραφος 1 στοιχείο δ) του δημοσιονομικού κανονισμού.

Στήριξη με τη μορφή επιχορηγήσεων για τον μηχανισμό έκτακτης ανάγκης στον κυβερνοχώρο, όπως ορίζεται στο άρθρο 10 του κανονισμού XXXX, μπορεί να χορηγείται απευθείας από το ECCC στα κράτη μέλη χωρίς πρόσκληση υποβολής προτάσεων, σύμφωνα με το άρθρο 195 παράγραφος 1 στοιχείο δ) του δημοσιονομικού κανονισμού.

Για τις δράσεις που προσδιορίζονται στο άρθρο 10 παράγραφος 1 στοιχείο γ) του κανονισμού 202X/XXXX, το ECCC ενημερώνει την Επιτροπή και τον ENISA σχετικά με τα αιτήματα των κρατών μελών για άμεσες επιχορηγήσεις χωρίς πρόσκληση υποβολής προτάσεων.

Για τη στήριξη της αμοιβαίας συνδρομής για την αντιμετώπιση σημαντικού ή μεγάλης κλίμακας περιστατικού στον τομέα της κυβερνοασφάλειας, όπως ορίζεται στο άρθρο 10 στοιχείο γ) του κανονισμού XXXX, και σύμφωνα με το άρθρο 193 παράγραφος 2

δεύτερο εδάφιο στοιχείο α) του δημοσιονομικού κανονισμού, σε δεόντως αιτιολογημένες περιπτώσεις, οι δαπάνες μπορούν να θεωρηθούν επιλέξιμες ακόμη και αν πραγματοποιήθηκαν πριν από την υποβολή της αίτησης επιχορήγησης.»·

6) τα παραρτήματα I και II τροποποιούνται σύμφωνα με το παράρτημα του παρόντος κανονισμού.

*Άρθρο 20*

**Αξιολόγηση**

Έως [τέσσερα έτη μετά την ημερομηνία εφαρμογής του παρόντος κανονισμού], η Επιτροπή υποβάλλει στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο εκθέσεις σχετικά με την αξιολόγηση και την επανεξέταση του παρόντος κανονισμού.

*Άρθρο 21*

**Διαδικασία επιτροπής**

1. Η Επιτροπή επικουρείται από την επιτροπή συντονισμού του προγράμματος «Ψηφιακή Ευρώπη» που συστάθηκε με τον κανονισμό (ΕΕ) 2021/694. Πρόκειται για επιτροπή κατά την έννοια του κανονισμού (ΕΕ) αριθ. 182/2011.
2. Όταν γίνεται παραπομπή στην παρούσα παράγραφο, εφαρμόζεται το άρθρο 5 του κανονισμού (ΕΕ) αριθ. 182/2011.

*Άρθρο 22*

**Έναρξη ισχύος**

Ο παρών κανονισμός αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή του στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Ο παρών κανονισμός είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος.

Στρασβούργο,

| | |
|---|---|
| *Για το Ευρωπαϊκό Κοινοβούλιο* | *Για το Συμβούλιο* |
| *Η Πρόεδρος* | *Ο Πρόεδρος* |

# ΝΟΜΟΘΕΤΙΚΟ ΔΗΜΟΣΙΟΝΟΜΙΚΟ ΔΕΛΤΙΟ

## 1. ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

**1.1. Τίτλος της πρότασης/πρωτοβουλίας**

**1.2. Σχετικοί τομείς πολιτικής**

**1.3. Η πρόταση/πρωτοβουλία αφορά:**

**1.4. Στόχοι**

*1.4.1. Γενικοί στόχοι*

*1.4.2. Ειδικοί στόχοι*

*1.4.3. Αναμενόμενα αποτελέσματα και επιπτώσεις*

*1.4.4. Δείκτες επιδόσεων*

**1.5. Αιτιολόγηση της πρότασης/πρωτοβουλίας**

*1.5.1. Βραχυπρόθεσμη ή μακροπρόθεσμη κάλυψη αναγκών, συμπεριλαμβανομένου λεπτομερούς χρονοδιαγράμματος για τη σταδιακή υλοποίηση της πρωτοβουλίας*

*1.5.2. Προστιθέμενη αξία της ενωσιακής παρέμβασης (που μπορεί να προκύπτει από διάφορους παράγοντες, π.χ. οφέλη από τον συντονισμό, ασφάλεια δικαίου, μεγαλύτερη αποτελεσματικότητα ή συμπληρωματικότητα). Για τους σκοπούς του παρόντος σημείου, «προστιθέμενη αξία της ενωσιακής παρέμβασης» είναι η αξία που απορρέει από την ενωσιακή παρέμβαση και η οποία προστίθεται στην αξία που θα είχε δημιουργηθεί αν τα κράτη μέλη ενεργούσαν μεμονωμένα.*

*1.5.3. Διδάγματα από ανάλογες εμπειρίες του παρελθόντος*

*1.5.4. Συμβατότητα με το πολυετές δημοσιονομικό πλαίσιο και ενδεχόμενες συνέργειες με άλλα κατάλληλα μέσα*

*1.5.5. Αξιολόγηση των διαφόρων διαθέσιμων επιλογών χρηματοδότησης, συμπεριλαμβανομένων των δυνατοτήτων ανακατανομής*

**1.6. Διάρκεια και δημοσιονομικές επιπτώσεις της πρότασης/πρωτοβουλίας**

**1.7. Προβλεπόμενες μέθοδοι εκτέλεσης του προϋπολογισμού**

## 2. ΜΕΤΡΑ ΔΙΑΧΕΙΡΙΣΗΣ

**2.1. Κανόνες παρακολούθησης και υποβολής εκθέσεων**

**2.2. Συστήματα διαχείρισης και ελέγχου**

*2.2.1. Αιτιολόγηση των τρόπων διαχείρισης, των μηχανισμών εκτέλεσης της χρηματοδότησης, των όρων πληρωμής και της προτεινόμενης στρατηγικής ελέγχου*

*2.2.2. Πληροφορίες σχετικά με τους κινδύνους που έχουν εντοπιστεί και τα συστήματα εσωτερικού ελέγχου που έχουν δημιουργηθεί για τον μετριασμό τους*

*2.2.3. Εκτίμηση και αιτιολόγηση της οικονομικής αποδοτικότητας των ελέγχων (λόγος του κόστους του ελέγχου προς την αξία των σχετικών κονδυλίων που αποτελούν αντικείμενο διαχείρισης) και αξιολόγηση του εκτιμώμενου επιπέδου κινδύνου σφάλματος (κατά την πληρωμή και κατά το κλείσιμο)*

**2.3. Μέτρα για την πρόληψη περιπτώσεων απάτης και παρατυπίας**

**3. ΕΚΤΙΜΩΜΕΝΕΣ ΔΗΜΟΣΙΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ**

**3.1. Τομείς του πολυετούς δημοσιονομικού πλαισίου και γραμμές δαπανών του προϋπολογισμού που επηρεάζονται**

**3.2. Εκτιμώμενες δημοσιονομικές επιπτώσεις της πρότασης στις πιστώσεις**

*3.2.1. Συνοπτική παρουσίαση των εκτιμώμενων επιπτώσεων στις επιχειρησιακές πιστώσεις*

*3.2.2. Εκτιμώμενο αποτέλεσμα που χρηματοδοτείται με επιχειρησιακές πιστώσεις*

*3.2.3. Συνοπτική παρουσίαση των εκτιμώμενων επιπτώσεων στις διοικητικές πιστώσεις*

*3.2.3.1. Εκτιμώμενες ανάγκες σε ανθρώπινους πόρους*

*3.2.4. Συμβατότητα με το ισχύον πολυετές δημοσιονομικό πλαίσιο*

*3.2.5. Συμμετοχή τρίτων στη χρηματοδότηση*

**3.3. Εκτιμώμενες επιπτώσεις στα έσοδα**

## 1. ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

### 1.1. Τίτλος της πρότασης/πρωτοβουλίας

Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τον καθορισμό μέτρων για την ενίσχυση της αλληλεγγύης και των ικανοτήτων της Ένωσης για την ανίχνευση, την προετοιμασία και την αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας

### 1.2. Σχετικοί τομείς πολιτικής

Μια Ευρώπη έτοιμη για την ψηφιακή εποχή

Ευρωπαϊκές στρατηγικές επενδύσεις

Δραστηριότητα: Διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης.

### 1.3. Η πρόταση/πρωτοβουλία αφορά:

☒ **νέα δράση**

☐ **νέα δράση έπειτα από δοκιμαστικό σχέδιο / προπαρασκευαστική ενέργεια**[33]

☐ **την παράταση υφιστάμενης δράσης**

☐ **συγχώνευση ή αναπροσανατολισμό μίας ή περισσότερων δράσεων προς άλλη/νέα δράση**

### 1.4. Στόχοι

*1.4.1. Γενικοί στόχοι*

Η πράξη για την αλληλεγγύη στον κυβερνοχώρο θα ενισχύσει την αλληλεγγύη σε επίπεδο Ένωσης για την καλύτερη ανίχνευση, προετοιμασία και αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας. Η πράξη αποσκοπεί:

α) στην ενίσχυση της κοινής ενωσιακής ανίχνευσης και αντίληψης της κατάστασης όσον αφορά τις απειλές και τα περιστατικά στον κυβερνοχώρο,

β) στην ενίσχυση της ετοιμότητας των κρίσιμων οντοτήτων σε ολόκληρη την ΕΕ και στην ενίσχυση της αλληλεγγύης με την ανάπτυξη κοινών ικανοτήτων αντιμετώπισης σημαντικών ή μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας, μεταξύ άλλων με την εξασφάλιση στήριξης για την αντιμετώπιση περιστατικών σε τρίτες χώρες συνδεδεμένες με το πρόγραμμα «Ψηφιακή Ευρώπη»,

γ) στην ενίσχυση της ανθεκτικότητας της Ένωσης και στη συμβολή στην αποτελεσματική αντίδραση με την εξέταση και την αξιολόγηση σημαντικών ή μεγάλης κλίμακας περιστατικών, συμπεριλαμβανομένης της άντλησης διδαγμάτων και, κατά περίπτωση, συστάσεων.

*1.4.2. Ειδικοί στόχοι*

Η πράξη για την αλληλεγγύη στον κυβερνοχώρο θα επιτύχει το σύνολο των στόχων μέσω:

[33] Όπως αναφέρεται στο άρθρο 58 παράγραφος 2 στοιχείο α) ή β) του δημοσιονομικού κανονισμού.

α) της ανάπτυξης πανευρωπαϊκής υποδομής κέντρων επιχειρήσεων ασφάλειας (ευρωπαϊκή κυβερνοασπίδα) για την οικοδόμηση και ενίσχυση κοινών ικανοτήτων ανίχνευσης και αντίληψης της κατάστασης·

β) της δημιουργίας μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο με σκοπό τη στήριξη των κρατών μελών όσον αφορά την προετοιμασία, την αντιμετώπιση και την άμεση ανάκαμψη από σημαντικά και μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας. Η στήριξη για την αντιμετώπιση περιστατικών διατίθεται επίσης στα ευρωπαϊκά θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης (EUIBA).

Οι εν λόγω δράσεις θα στηριχθούν με χρηματοδότηση από το πρόγραμμα «Ψηφιακή Ευρώπη», το οποίο θα τροποποιηθεί με την παρούσα νομοθετική πράξη προκειμένου να καθοριστούν οι προαναφερθείσες δράσεις, να παρασχεθεί χρηματοδοτική στήριξη για την ανάπτυξή τους και να αποσαφηνιστούν οι προϋποθέσεις για τη χορήγηση χρηματοδοτικής στήριξης·

γ) της δημιουργίας ενός ευρωπαϊκού μηχανισμού εξέτασης περιστατικών κυβερνοασφάλειας για την εξέταση και την αξιολόγηση σημαντικών ή μεγάλης κλίμακας περιστατικών.

*1.4.3. Αναμενόμενα αποτελέσματα και επιπτώσεις*

*Να προσδιοριστούν τα αποτελέσματα που θα πρέπει να έχει η πρόταση/πρωτοβουλία όσον αφορά τους στοχοθετημένους δικαιούχους / τις στοχοθετημένες ομάδες.*

Η πρόταση θα αποφέρει σημαντικά οφέλη στα διάφορα ενδιαφερόμενα μέρη. Η ευρωπαϊκή κυβερνοασπίδα θα βελτιώσει τις ικανότητες των κρατών μελών όσον αφορά την ανίχνευση κυβερνοαπειλών. Ο μηχανισμός έκτακτης ανάγκης στον κυβερνοχώρο θα συμπληρώσει τις δράσεις των κρατών μελών μέσω στήριξης έκτακτης ανάγκης για ετοιμότητα, αντιμετώπιση και άμεση ανάκαμψη/αποκατάσταση της λειτουργίας βασικών υπηρεσιών.

Οι εν λόγω δράσεις θα ενισχύσουν την ανταγωνιστική θέση της βιομηχανίας και των υπηρεσιών στην Ευρώπη σε ολόκληρη την ψηφιοποιημένη οικονομία και θα στηρίξουν τον ψηφιακό μετασχηματισμό τους, με την ενίσχυση του επιπέδου κυβερνοασφάλειας στην ψηφιακή ενιαία αγορά. Ειδικότερα, αποσκοπούν στην αύξηση της ανθεκτικότητας των πολιτών, των επιχειρήσεων και των οντοτήτων που δραστηριοποιούνται σε τομείς κρίσιμης ή εξαιρετικά κρίσιμης σημασίας έναντι των αυξανόμενων απειλών κυβερνοασφάλειας, οι οποίες μπορεί να έχουν καταστροφικές κοινωνικές και οικονομικές επιπτώσεις. Για τον σκοπό αυτό, θα πραγματοποιηθούν επενδύσεις σε εργαλεία που θα στηρίξουν την ταχύτερη ανίχνευση και αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας και θα βοηθήσουν τα κράτη μέλη να προετοιμαστούν και να αντιμετωπίζουν καλύτερα σημαντικά και μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας. Θα πρέπει επίσης να στηριχθεί η αύξηση των ικανοτήτων της Ένωσης σε αυτούς τους τομείς, ιδίως όσον αφορά τη συλλογή και ανάλυση δεδομένων σχετικά με απειλές και περιστατικά κυβερνοασφάλειας.

*1.4.4. Δείκτες επιδόσεων*

*Να προσδιοριστούν οι δείκτες για την παρακολούθηση της προόδου και των επιτευγμάτων.*

Προκειμένου να προωθηθεί η αλληλεγγύη σε επίπεδο Ένωσης, μπορούν να ληφθούν υπόψη διάφοροι δείκτες:

1) ο αριθμός υποδομών ή εργαλείων κυβερνοασφάλειας, ή και τα δύο, που αποκτώνται με κοινές συμβάσεις·

2) ο αριθμός των δράσεων που στηρίζουν την ετοιμότητα και την αντιμετώπιση περιστατικών κυβερνοασφάλειας στο πλαίσιο του μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο.

**1.5. Αιτιολόγηση της πρότασης/πρωτοβουλίας**

*1.5.1. Βραχυπρόθεσμη ή μακροπρόθεσμη κάλυψη αναγκών, συμπεριλαμβανομένου λεπτομερούς χρονοδιαγράμματος για τη σταδιακή υλοποίηση της πρωτοβουλίας*

Ο κανονισμός θα πρέπει να εφαρμοστεί πλήρως σε σύντομο χρονικό διάστημα μετά την έκδοσή του, δηλαδή την εικοστή ημέρα μετά τη δημοσίευσή του στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

*1.5.2. Προστιθέμενη αξία της ενωσιακής παρέμβασης (που μπορεί να προκύπτει από διάφορους παράγοντες, π.χ. οφέλη από τον συντονισμό, ασφάλεια δικαίου, μεγαλύτερη αποτελεσματικότητα ή συμπληρωματικότητα). Για τους σκοπούς του παρόντος σημείου, «προστιθέμενη αξία της ενωσιακής παρέμβασης» είναι η αξία που απορρέει από την ενωσιακή παρέμβαση και η οποία προστίθεται στην αξία που θα είχε δημιουργηθεί αν τα κράτη μέλη ενεργούσαν μεμονωμένα.*

Ο ισχυρός διασυνοριακός χαρακτήρας των απειλών κυβερνοασφάλειας εν γένει, καθώς και ο αυξανόμενος αριθμός των κινδύνων και των περιστατικών, τα οποία έχουν δευτερογενείς επιπτώσεις σε διασυνοριακό επίπεδο, καθώς και σε τομείς και προϊόντα, συνεπάγονται ότι οι στόχοι της παρούσας παρέμβασης δεν μπορούν να επιτευχθούν αποτελεσματικά μόνο από τα κράτη μέλη και ότι απαιτείται κοινή δράση και αλληλεγγύη σε επίπεδο Ένωσης. Η εμπειρία από την αντιμετώπιση των κυβερνοαπειλών που απορρέουν από τον πόλεμο κατά της Ουκρανίας, σε συνδυασμό με τα διδάγματα που αντλήθηκαν από μια άσκηση κυβερνοασφάλειας που διεξήχθη υπό τη γαλλική Προεδρία (EU CyCLES), έδειξε ότι θα πρέπει να αναπτυχθούν συγκεκριμένοι μηχανισμοί αμοιβαίας στήριξης, ιδίως η συνεργασία με τον ιδιωτικό τομέα, για την επίτευξη αλληλεγγύης σε επίπεδο ΕΕ. Στο πλαίσιο αυτό, στα συμπεράσματα της 23ης Μαΐου 2022 σχετικά με τη διαμόρφωση της στάσης της Ευρωπαϊκής Ένωσης στον κυβερνοχώρο, το Συμβούλιο καλεί την Επιτροπή να υποβάλει πρόταση για ένα νέο ταμείο αντιμετώπισης καταστάσεων έκτακτης ανάγκης στον τομέα της κυβερνοασφάλειας. Η στήριξη και οι δράσεις σε επίπεδο Ένωσης για την καλύτερη ανίχνευση των απειλών κυβερνοασφάλειας και την αύξηση των ικανοτήτων ετοιμότητας και αντίδρασης παρέχουν προστιθέμενη αξία, διότι αποφεύγεται η αλληλεπικάλυψη προσπαθειών σε ολόκληρη την Ένωση και τα κράτη μέλη. Θα οδηγήσουν σε καλύτερη αξιοποίηση των υφιστάμενων πάγιων στοιχείων και σε μεγαλύτερο συντονισμό και ανταλλαγή πληροφοριών σχετικά με τα διδάγματα που αντλήθηκαν.

*1.5.3. Διδάγματα από ανάλογες εμπειρίες του παρελθόντος*

Όσον αφορά την αντίληψη της κατάστασης και την ανίχνευση στο πλαίσιο της ευρωπαϊκής κυβερνοασπίδας, πραγματοποιήθηκε, στο πλαίσιο του προγράμματος εργασίας για την κυβερνοασφάλεια της περιόδου 2021-2022 βάσει του προγράμματος «Ψηφιακή Ευρώπη», πρόσκληση εκδήλωσης ενδιαφέροντος για την από κοινού προμήθεια εργαλείων και υποδομών για τη δημιουργία διασυνοριακών SOC, καθώς και πρόσκληση για επιχορηγήσεις ώστε να καταστεί δυνατή η ανάπτυξη ικανοτήτων των SOC που εξυπηρετούν δημόσιους και ιδιωτικούς οργανισμούς.

Όσον αφορά την ετοιμότητα και την αντιμετώπιση περιστατικών, η Επιτροπή έχει καταρτίσει βραχυπρόθεσμο πρόγραμμα για τη στήριξη των κρατών μελών, μέσω πρόσθετης χρηματοδότησης που διατίθεται στον ENISA, με σκοπό την άμεση ενίσχυση της ετοιμότητας και των ικανοτήτων αντιμετώπισης σοβαρών περιστατικών στον κυβερνοχώρο. Οι καλυπτόμενες υπηρεσίες περιλαμβάνουν δράσεις ετοιμότητας, όπως δοκιμές διείσδυσης κρίσιμων οντοτήτων για τον εντοπισμό τρωτών σημείων. Επίσης, ενισχύει τις δυνατότητες παροχής βοήθειας στα κράτη μέλη σε περίπτωση σοβαρού περιστατικού που επηρεάζει κρίσιμες οντότητες. Η εφαρμογή αυτού του βραχυπρόθεσμου προγράμματος από τον ENISA είναι σε εξέλιξη και έχουν ήδη παρασχεθεί σχετικές πολύτιμες πληροφορίες που έχουν ληφθεί υπόψη κατά την προετοιμασία του παρόντος κανονισμού.

*1.5.4. Συμβατότητα με το πολυετές δημοσιονομικό πλαίσιο και ενδεχόμενες συνέργειες με άλλα κατάλληλα μέσα*

Η πράξη για την αλληλεγγύη στον κυβερνοχώρο θα βασιστεί σε δράσεις που υποστηρίζονται επί του παρόντος από την Ένωση και τα κράτη μέλη για την ενίσχυση της αντίληψης της κατάστασης και της ανίχνευσης κυβερνοαπειλών, καθώς και για την αντιμετώπιση μεγάλης κλίμακας και διασυνοριακών περιστατικών στον τομέα της κυβερνοασφάλειας. Επιπλέον, το μέσο συνάδει με άλλα πλαίσια διαχείρισης κρίσεων, συμπεριλαμβανομένων των IPCR, της κοινής πολιτικής ασφάλειας και άμυνας, συμπεριλαμβανομένων των ομάδων ταχείας αντίδρασης στον κυβερνοχώρο, και της συνδρομής που παρέχεται από ένα κράτος μέλος σε άλλο κράτος μέλος στο πλαίσιο του άρθρου 42 παράγραφος 7 της Συνθήκης για την Ευρωπαϊκή Ένωση. Η νέα πρόταση θα συμπληρώσει και θα στηρίξει επίσης τις δομές που αναπτύσσονται στο πλαίσιο άλλων μέσων κυβερνοασφάλειας, όπως η οδηγία (ΕΕ) 2022/2555 (οδηγία NIS2) ή ο κανονισμός 2019/881 (πράξη για την κυβερνοασφάλεια).

*1.5.5. Αξιολόγηση των διαφόρων διαθέσιμων επιλογών χρηματοδότησης, συμπεριλαμβανομένων των δυνατοτήτων ανακατανομής*

Η διαχείριση των τομέων δράσης που ανατίθενται στον ENISA ανταποκρίνεται στην υφιστάμενη εντολή και στα γενικά καθήκοντά του. Οι εν λόγω τομείς δράσης ενδέχεται να απαιτούν ειδικά προφίλ ή νέες αναθέσεις, αλλά αυτές μπορούν να απορροφηθούν από τους υφιστάμενους πόρους του ENISA και να επιλυθούν μέσω ανακατανομής ή σύνδεσης διαφόρων αναθέσεων. Ο ENISA εφαρμόζει επί του παρόντος ένα βραχυπρόθεσμο πρόγραμμα που θεσπίστηκε το 2022 από την Επιτροπή για την άμεση ενίσχυση της ετοιμότητας και των ικανοτήτων αντιμετώπισης σοβαρών περιστατικών στον κυβερνοχώρο. Οι καλυπτόμενες υπηρεσίες περιλαμβάνουν δυνατότητες παροχής βοήθειας στα κράτη μέλη σε περίπτωση σοβαρού περιστατικού που επηρεάζει κρίσιμες οντότητες. Η εφαρμογή αυτού του βραχυπρόθεσμου προγράμματος από τον ENISA βρίσκεται σε εξέλιξη και έχει ήδη παράσχει σχετικές πολύτιμες πληροφορίες που έχουν ληφθεί υπόψη κατά την προετοιμασία του παρόντος κανονισμού. Οι πόροι που διατίθενται για το βραχυπρόθεσμο πρόγραμμα μπορούν επίσης να χρησιμοποιηθούν στο πλαίσιο του παρόντος κανονισμού.

**1.6. Διάρκεια και δημοσιονομικές επιπτώσεις της πρότασης/πρωτοβουλίας**

☒ **περιορισμένη διάρκεια**

– ☒ σε ισχύ από την ημερομηνία έγκρισης της πρότασης κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ενίσχυση της αλληλεγγύης και των ικανοτήτων της Ένωσης για την ανίχνευση, την προετοιμασία και την αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας (στο εξής: πράξη για την αλληλεγγύη στον κυβερνοχώρο)

– ☒ δημοσιονομικές επιπτώσεις από το 2023 έως το 2027 για πιστώσεις ανάληψης υποχρεώσεων και από το 2023 έως το 2031 για πιστώσεις πληρωμών[34].

☐ **απεριόριστη διάρκεια**

– Περίοδος σταδιακής εφαρμογής από το ΕΕΕΕ έως το ΕΕΕΕ,

– και στη συνέχεια πλήρης εφαρμογή.

**1.7. Προβλεπόμενες μέθοδοι εκτέλεσης του προϋπολογισμού[35]**

☒ **Άμεση διαχείριση** από την Επιτροπή

– ☒ από τις υπηρεσίες της, συμπεριλαμβανομένου του προσωπικού της στις αντιπροσωπείες της Ένωσης

– ☐ από τους εκτελεστικούς οργανισμούς

☐ **Επιμερισμένη διαχείριση** με τα κράτη μέλη

☒ **Έμμεση διαχείριση** με ανάθεση καθηκόντων εκτέλεσης του προϋπολογισμού:

– ☐ σε τρίτες χώρες ή οργανισμούς που αυτές έχουν ορίσει·

– ☐ σε διεθνείς οργανισμούς και στις οργανώσεις τους (να προσδιοριστούν)·

– ☐ στην ΕΤΕπ και στο Ευρωπαϊκό Ταμείο Επενδύσεων·

– ☒ στους οργανισμούς που αναφέρονται στα άρθρα 70 και 71 του δημοσιονομικού κανονισμού·

– ☐ σε οργανισμούς δημοσίου δικαίου·

– ☐ σε οργανισμούς που διέπονται από ιδιωτικό δίκαιο και έχουν αποστολή δημόσιας υπηρεσίας, στον βαθμό που παρέχουν επαρκείς οικονομικές εγγυήσεις·

– ☐ σε οργανισμούς που διέπονται από το ιδιωτικό δίκαιο κράτους μέλους, στους οποίους έχει ανατεθεί η εκτέλεση σύμπραξης δημόσιου και ιδιωτικού τομέα και οι οποίοι παρέχουν επαρκείς οικονομικές εγγυήσεις·

– ☐ σε οργανισμούς ή πρόσωπα επιφορτισμένα με την εφαρμογή συγκεκριμένων δράσεων στην ΚΕΠΠΑ βάσει του τίτλου V της ΣΕΕ και τα οποία προσδιορίζονται στην αντίστοιχη βασική πράξη.

– *Αν αναφέρονται περισσότεροι του ενός τρόποι διαχείρισης, να διευκρινιστούν στο τμήμα «Παρατηρήσεις».*

Παρατηρήσεις

---

34 Οι δράσεις της πράξης θα πρέπει να στηριχθούν από το επόμενο πολυετές δημοσιονομικό πλαίσιο.

35 Οι λεπτομέρειες σχετικά με τις μεθόδους εκτέλεσης του προϋπολογισμού, καθώς και οι παραπομπές στον δημοσιονομικό κανονισμό, είναι διαθέσιμες στον ιστότοπο BUDGpedia: https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx.

Οι δράσεις που σχετίζονται με την ευρωπαϊκή κυβερνοασπίδα θα υλοποιηθούν από το ECCC. Έως ότου το ECCC αποκτήσει την ικανότητα εκτέλεσης του προϋπολογισμού του, η Ευρωπαϊκή Επιτροπή θα υλοποιήσει τις δράσεις υπό άμεση διαχείριση εξ ονόματος του ECCC. Το ECCC μπορεί να επιλέγει οντότητες βάσει προσκλήσεων εκδήλωσης ενδιαφέροντος για συμμετοχή σε κοινές προμήθειες εργαλείων. Το ECCC μπορεί να χορηγεί επιχορηγήσεις για τη λειτουργία αυτών των εργαλείων.

Επιπλέον, το ECCC μπορεί να χορηγεί επιχορηγήσεις για δράσεις ετοιμότητας στο πλαίσιο του μηχανισμού έκτακτης ανάγκης για την κυβερνοασφάλεια.

Η Επιτροπή έχει τη συνολική ευθύνη για την υλοποίηση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. Η Επιτροπή μπορεί να αναθέσει στον ENISA, εν όλω ή εν μέρει, μέσω συμφωνιών συνεισφοράς, τη λειτουργία και τη διαχείριση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. Οι δράσεις που ανατίθενται στον ENISA βάσει του παρόντος κανονισμού συνάδουν με την υφιστάμενη εντολή του. Σε αυτές τις δράσεις περιλαμβάνονται: i) υποστήριξη της ομάδας συνεργασίας NIS για την ανάπτυξη των δράσεων ετοιμότητας σύμφωνα με τις εκτιμήσεις κινδύνου, ii) υποστήριξη της Επιτροπής για τη θέσπιση και την εποπτεία της υλοποίησης της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, συμπεριλαμβανομένης της λήψης και της επεξεργασίας των αιτημάτων στήριξης, iii) ανάπτυξη υποδειγμάτων για τη διευκόλυνση της υποβολής αιτημάτων στήριξης και ειδικών συμφωνιών που πρόκειται να συναφθούν μεταξύ του παρόχου υπηρεσιών και του χρήστη στον οποίο παρέχεται η στήριξη στο πλαίσιο της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, iv) εξέταση και αξιολόγηση απειλών, τρωτών σημείων και δράσεων μετριασμού σε σχέση με συγκεκριμένα σημαντικά ή μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας και εκπόνηση σχετικών εκθέσεων.

Όλες αυτές οι εργασίες εκτιμώνται σε περίπου 7 ΙΠΑ από τους υφιστάμενους πόρους του ENISA, με βάση την ήδη υπάρχουσα εμπειρογνωσία και τις προπαρασκευαστικές εργασίες που πραγματοποιεί επί του παρόντος ο ENISA στο πλαίσιο της πιλοτικής εφαρμογής της στήριξης της ετοιμότητας και της αντιμετώπισης περιστατικών.

## 2. ΜΕΤΡΑ ΔΙΑΧΕΙΡΙΣΗΣ

### 2.1. Κανόνες παρακολούθησης και υποβολής εκθέσεων

*Να προσδιοριστούν η συχνότητα και οι όροι.*

Η Επιτροπή θα παρακολουθεί την υλοποίηση, την εφαρμογή και τη συμμόρφωση προς τις νέες αυτές διατάξεις με σκοπό την αξιολόγηση της αποτελεσματικότητάς τους. Η Επιτροπή υποβάλλει έκθεση σχετικά με την αξιολόγηση και την επανεξέταση του παρόντος κανονισμού στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο εντός τεσσάρων ετών από την ημερομηνία εφαρμογής του.

### 2.2. Συστήματα διαχείρισης και ελέγχου

*2.2.1. Αιτιολόγηση των τρόπων διαχείρισης, των μηχανισμών εκτέλεσης της χρηματοδότησης, των όρων πληρωμής και της προτεινόμενης στρατηγικής ελέγχου*

Ο κανονισμός θεσπίζει πλαίσιο για την εκτέλεση της χρηματοδότησης της ΕΕ με σκοπό την αύξηση της ανθεκτικότητας στον τομέα της κυβερνοασφάλειας μέσω δράσεων που ενισχύουν τις ικανότητες ανίχνευσης, αντιμετώπισης και ανάκαμψης σε περίπτωση σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας. Η Διοικητικές Μονάδες εντός της ΓΔ CNECT που είναι αρμόδιες για τον τομέα πολιτικής θα διαχειρίζεται την εφαρμογή της οδηγίας.

Για την εκτέλεση των νέων καθηκόντων, είναι απαραίτητο να παρασχεθούν κατάλληλοι πόροι στις υπηρεσίες της Επιτροπής. Η επιβολή του νέου κανονισμού εκτιμάται ότι απαιτεί 6 ΙΠΑ (3 AD και 3 AC) για την κάλυψη των ακόλουθων καθηκόντων:

- τον καθορισμό δράσεων ετοιμότητας σύμφωνα με τις εκτιμήσεις κινδύνου·
- τη διασφάλιση της διαλειτουργικότητας μεταξύ των διασυνοριακών πλατφορμών SOC·
- την εκπόνηση πιθανών εκτελεστικών πράξεων (δύο για τα SOC και δύο για τον μηχανισμό έκτακτης ανάγκης για την κυβερνοασφάλεια)·
- τη διαχείριση των συμφωνιών υποδοχής και χρήσης για τα SOC·
- τη δημιουργία και διαχείριση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, απευθείας ή μέσω συμφωνίας συνεισφοράς με τον ENISA. Σε περίπτωση συμφωνίας συνεισφοράς με τον ENISA, την εκπόνηση και εποπτεία της εφαρμογής της συμφωνίας συνεισφοράς για τα καθήκοντα που ανατίθενται στον ENISA·
- τη συμμετοχή στις ομάδες διαβούλευσης που συγκαλεί ο ENISA για την εξέταση και την αξιολόγηση σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας και την εκπόνηση των εκθέσεων.

*2.2.2. Πληροφορίες σχετικά με τους κινδύνους που έχουν εντοπιστεί και τα συστήματα εσωτερικού ελέγχου που έχουν δημιουργηθεί για τον μετριασμό τους*

Ένας κίνδυνος που έχει εντοπιστεί για την ευρωπαϊκή κυβερνοασπίδα είναι ότι τα κράτη μέλη δεν ανταλλάσσουν επαρκή όγκο σχετικών πληροφοριών για κυβερνοαπειλές είτε εντός των διασυνοριακών πλατφορμών SOC είτε μεταξύ διασυνοριακών πλατφορμών και άλλων σχετικών οντοτήτων σε επίπεδο ΕΕ. Προκειμένου να μετριαστούν οι κίνδυνοι αυτοί, η κατανομή της χρηματοδότησης θα

πραγματοποιηθεί κατόπιν πρόσκλησης εκδήλωσης ενδιαφέροντος στο πλαίσιο της οποίας τα κράτη μέλη θα δεσμευτούν να ανταλλάσσουν ορισμένο όγκο πληροφοριών με φορείς στο επίπεδο της ΕΕ. Στη συνέχεια, η δέσμευση αυτή θα επισημοποιηθεί με τη μορφή συμφωνίας υποδοχής και χρήσης, η οποία θα παρέχει στο ECCC την εξουσία να διενεργεί ελέγχους για να διασφαλίζει ότι τα εργαλεία και οι υποδομές που αποτελούν αντικείμενο κοινής διαδικασίας προμήθειας χρησιμοποιούνται σύμφωνα με τη συμφωνία. Οι δεσμεύσεις για υψηλό επίπεδο ανταλλαγής πληροφοριών στο πλαίσιο των διασυνοριακών SOC θα επισημοποιηθούν με τη μορφή συμφωνίας κοινοπραξίας.

Ένας κίνδυνος που εντοπίστηκε όσον αφορά τον μηχανισμό έκτακτης ανάγκης στον κυβερνοχώρο είναι ότι οι χρήστες που συμμετέχουν στον μηχανισμό δεν λαμβάνουν επαρκή μέτρα για τη διασφάλιση της ετοιμότητας έναντι κυβερνοεπιθέσεων. Για τον λόγο αυτό, για να μπορούν να λαμβάνουν στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, οι χρήστες υποχρεούνται να λαμβάνουν τέτοια μέτρα ετοιμότητας. Κατά την υποβολή των αιτημάτων στήριξης στην εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, οι χρήστες πρέπει να εξηγούν ποια μέτρα έχουν ήδη ληφθεί για την αντιμετώπιση του περιστατικού, τα οποία θα λαμβάνονται υπόψη κατά την αξιολόγηση των αιτημάτων προς την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας.

*2.2.3. Εκτίμηση και αιτιολόγηση της οικονομικής αποδοτικότητας των ελέγχων (λόγος του κόστους του ελέγχου προς την αξία των σχετικών κονδυλίων που αποτελούν αντικείμενο διαχείρισης) και αξιολόγηση του εκτιμώμενου επιπέδου κινδύνου σφάλματος (κατά την πληρωμή και κατά το κλείσιμο)*

Λαμβανομένου υπόψη ότι οι κανόνες συμμετοχής στο πρόγραμμα «Ψηφιακή Ευρώπη» που εφαρμόζονται όσον αφορά τη στήριξη στο πλαίσιο της πράξης για την αλληλεγγύη στον κυβερνοχώρο είναι παρόμοιοι με τους κανόνες που θα χρησιμοποιήσει η Επιτροπή στα προγράμματα εργασίας της, και δεδομένου ότι ο πληθυσμός των δικαιούχων παρουσιάζει παρεμφερή χαρακτηριστικά κινδύνου με εκείνα των προγραμμάτων υπό άμεση διαχείριση, αναμένεται ευλόγως ότι και το περιθώριο σφάλματος θα είναι παρόμοιο με εκείνο που έχει προβλέψει η Επιτροπή για το πρόγραμμα «Ψηφιακή Ευρώπη», δηλαδή θα παρέχει εύλογη βεβαιότητα ότι ο κίνδυνος σφάλματος κατά τη διάρκεια της πολυετούς περιόδου δαπανών θα βρίσκεται, σε ετήσια βάση, εντός των ορίων 2-5 %, με απώτερο σκοπό να επιτευχθεί εναπομένον ποσοστό σφάλματος όσο το δυνατόν πλησιέστερα στο 2 % κατά το κλείσιμο των πολυετών προγραμμάτων, αφού θα έχει συνεκτιμηθεί ο δημοσιονομικός αντίκτυπος όλων των ελέγχων και των μέτρων διόρθωσης και ανάκτησης.

## 2.3. Μέτρα για την πρόληψη περιπτώσεων απάτης και παρατυπίας

*Να προσδιοριστούν τα ισχύοντα ή τα προβλεπόμενα μέτρα πρόληψης και προστασίας, π.χ. στη στρατηγική για την καταπολέμηση της απάτης.*

Στην περίπτωση της ευρωπαϊκής κυβερνοασπίδας, το ECCC θα έχει την εξουσία να ελέγχει, βάσει πρόσβασης σε πληροφορίες και επιτόπιων ελέγχων, τα εργαλεία και τις υποδομές που αποτελούν αντικείμενο κοινής διαδικασίας προμήθειας, σύμφωνα με τη συμφωνία υποδοχής και χρήσης που θα υπογραφεί μεταξύ της κοινοπραξίας υποδοχής και του ECCC.

Τα ισχύοντα μέτρα πρόληψης περιπτώσεων απάτης που εφαρμόζονται στα ευρωπαϊκά θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης θα καλύπτουν τις πρόσθετες πιστώσεις που είναι αναγκαίες για τον παρόντα κανονισμό.

## 3. ΕΚΤΙΜΩΜΕΝΕΣ ΔΗΜΟΣΙΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

### 3.1. Τομείς του πολυετούς δημοσιονομικού πλαισίου και γραμμές δαπανών του προϋπολογισμού που επηρεάζονται

- Υφιστάμενες γραμμές του προϋπολογισμού

*Κατά σειρά τομέων του πολυετούς δημοσιονομικού πλαισίου και γραμμών του προϋπολογισμού.*

| Τομέας του πολυετούς δημοσιονομικού πλαισίου | Γραμμή του προϋπολογισμού | Είδος δαπάνης | Συμμετοχή | | | |
|---|---|---|---|---|---|---|
| | Αριθμός | ΔΠ/ΜΔΠ[36] | χωρών ΕΖΕΣ[37] | υποψηφίων για ένταξη χωρών και δυνάμει υποψηφίων χωρών[38] | άλλων τρίτων χωρών | άλλα έσοδα για ειδικό προορισμό |
| 1 | 02 04 01 10 – Πρόγραμμα «Ψηφιακή Ευρώπη» — Κυβερνοασφάλεια | ΔΠ | ΝΑΙ | ΝΑΙ | ΟΧΙ | ΟΧΙ |
| 1 | 02 04 01 11 – Πρόγραμμα «Ψηφιακή Ευρώπη» — Ευρωπαϊκό βιομηχανικό, τεχνολογικό και ερευνητικό κέντρο ικανοτήτων στον τομέα της κυβερνοασφάλειας | ΔΠ | ΝΑΙ | ΝΑΙ | ΟΧΙ | ΟΧΙ |
| 1 | 02 04 03 – Πρόγραμμα «Ψηφιακή Ευρώπη» — Τεχνητή νοημοσύνη | ΔΠ | ΝΑΙ | ΝΑΙ | ΟΧΙ | ΟΧΙ |
| 1 | 02 04 04 – Πρόγραμμα «Ψηφιακή Ευρώπη» — Δεξιότητες | ΔΠ | ΝΑΙ | ΝΑΙ | ΟΧΙ | ΟΧΙ |
| 1 | 02 01 30 — Δαπάνες στήριξης για το πρόγραμμα «Ψηφιακή Ευρώπη» | ΜΔΠ | ΝΑΙ | ΝΑΙ | ΟΧΙ | ΟΧΙ |

[36] ΔΠ = Διαχωριζόμενες πιστώσεις / ΜΔΠ = Μη διαχωριζόμενες πιστώσεις.

[37] ΕΖΕΣ: Ευρωπαϊκή Ζώνη Ελεύθερων Συναλλαγών.

[38] Οι υποψήφιες και, κατά περίπτωση, οι δυνητικά υποψήφιες χώρες.

### 3.2. Εκτιμώμενες δημοσιονομικές επιπτώσεις της πρότασης στις πιστώσεις

*3.2.1. Συνοπτική παρουσίαση των εκτιμώμενων επιπτώσεων στις επιχειρησιακές πιστώσεις*

– ☐ Η πρόταση/πρωτοβουλία δεν συνεπάγεται τη χρησιμοποίηση επιχειρησιακών πιστώσεων

– ☒ Η πρόταση/πρωτοβουλία συνεπάγεται τη χρησιμοποίηση επιχειρησιακών πιστώσεων, όπως εξηγείται κατωτέρω.

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

| **Τομέας του πολυετούς δημοσιονομικού πλαισίου** | Αριθμός | 1 **Ενιαία αγορά, καινοτομία και ψηφιακή οικονομία** |
|---|---|---|

Η πρόταση δεν θα αυξήσει το συνολικό επίπεδο των αναλήψεων υποχρεώσεων στο πλαίσιο του προγράμματος «Ψηφιακή Ευρώπη». Πράγματι, η συμβολή στην πρωτοβουλία αυτή είναι η ανακατανομή των αναλήψεων υποχρεώσεων που προέρχονται από το SO2 και το SO4 για την ενίσχυση του προϋπολογισμού του SO3 και του ECCC. Οποιαδήποτε αύξηση των αναλήψεων υποχρεώσεων στο πλαίσιο του προγράμματος «Ψηφιακή Ευρώπη» που προκύπτει από την αναθεώρηση του ΠΔΠ μπορεί να χρησιμοποιηθεί για τους σκοπούς της παρούσας πρωτοβουλίας.

| ΓΔ CONNECT | | | Έτος **2025** | Έτος **2026** | Έτος **2027** | Έτος **2028+** | Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6) | | | **ΣΥΝΟΛΟ** |
|---|---|---|---|---|---|---|---|---|---|---|
| ○ Επιχειρησιακές πιστώσεις | | | | | | | | | | |
| Γραμμή προϋπολογισμού[39] 02.040110 (ανακατανομή από το 02.0403 και το 02.0404) | Αναλήψεις υποχρεώσεων | (1α) | 15,000 | 15,000 | 6,000 | π.υ. | | | | **36,000** |
| | Πληρωμές | (2α) | 15,000 | 15,000 | 6,000 | | | | | **36,000** |
| Γραμμή προϋπολογισμού 02.040111.02 (ανακατανομή από το 02.0403 και το 02.0404) | Αναλήψεις υποχρεώσεων | (1β) | 13,000 | 23,000 | 28,000 | π.υ. | | | | **64,000** |
| | Πληρωμές | (2β) | 8,450 | 18,200 | 25,250 | 12,100 | | | | **64,000** |
| Πιστώσεις διοικητικού χαρακτήρα χρηματοδοτούμενες από το κονδύλιο ειδικών προγραμμάτων[40] | | | | | | | | | | |

[39] Σύμφωνα με την επίσημη ονοματολογία του προϋπολογισμού.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Γραμμή του προϋπολογισμού 02.0130 | | (3) | 0,150 | 0,150 | 0,150 | π.υ. | | | | 0,450 |
| **ΣΥΝΟΛΟ πιστώσεων για τη ΓΔ CONNECT** | Αναλήψεις υποχρεώσεων | =1α+1 β +3 | **28,150** | **38,150** | **34,150** | **π.υ.** | | | | **100,450** |
| | Πληρωμές | =2α+2 β +3 | **23,600** | **33,350** | **31,400** | **12,100** | | | | **100,450** |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ○ ΣΥΝΟΛΟ επιχειρησιακών πιστώσεων | Αναλήψεις υποχρεώσεων | (4) | 28,000 | 38,000 | 34,000 | π.υ. | | | | **100,000** |
| | Πληρωμές | (5) | 23,450 | 33,200 | 31,250 | 12,100 | | | | **100,000** |
| ○ ΣΥΝΟΛΟ πιστώσεων διοικητικού χαρακτήρα χρηματοδοτούμενων από το κονδύλιο ειδικών προγραμμάτων | | (6) | 0,150 | 0,150 | 0,150 | π.υ. | | | | **0,450** |
| **ΣΥΝΟΛΟ πιστώσεωντου ΤΟΜΕΑ 1** του πολυετούς δημοσιονομικού πλαισίου | Αναλήψεις υποχρεώσεων | =4+ 6 | **28,150** | **38,150** | **34,150** | **π.υ.** | | | | **100,450** |
| | Πληρωμές | =5+ 6 | **23,600** | **33,350** | **31,400** | **12,100** | | | | **100,450** |

**Αν η πρόταση/πρωτοβουλία επηρεάζει περισσότερους του ενός επιχειρησιακούς τομείς, επαναλάβετε το ανωτέρω τμήμα:**

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ○ ΣΥΝΟΛΟ επιχειρησιακών πιστώσεων (όλοι οι επιχειρησιακοί τομείς) | Αναλήψεις υποχρεώσεων | (4) | 28,000 | 38,000 | 34,000 | π.υ. | | | | **100,000** |
| | Πληρωμές | (5) | 23,450 | 33,200 | 31,250 | 12,100 | | | | **100,000** |
| ΣΥΝΟΛΟ πιστώσεων διοικητικού χαρακτήρα χρηματοδοτούμενων από το κονδύλιο ειδικών προγραμμάτων (όλοι οι επιχειρησιακοί τομείς) | | (6) | 0,150 | 0,150 | 0,150 | | | | | **0,450** |

[40] Τεχνική και/ή διοικητική βοήθεια και δαπάνες στήριξης της εφαρμογής προγραμμάτων και/ή δράσεων της ΕΕ (πρώην γραμμές «ΒΑ»), έμμεση έρευνα, άμεση έρευνα.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **ΣΥΝΟΛΟ πιστώσεωντων ΤΟΜΕΩΝ 1 έως 6**<br>του πολυετούς δημοσιονομικού πλαισίου<br><br>(Ποσό αναφοράς) | Αναλήψεις υποχρεώσεων | =4+ 6 | **28,150** | **38,150** | **34,150** | **π.υ.** | | | | **100,450** |
| | Πληρωμές | =5+ 6 | **23,600** | **33,350** | **31,400** | **12,100** | | | | **100,450** |

| **Τομέας του πολυετούςδημοσιονομικού πλαισίου** | **7** | «Διοικητικές δαπάνες» |
|---|---|---|

Αυτό το τμήμα θα πρέπει να συμπληρωθεί με «στοιχεία διοικητικού χαρακτήρα του προϋπολογισμού» τα οποία θα εισαχθούν, πρώτα, στο παράρτημα του νομοθετικού δημοσιονομικού δελτίου (παράρτημα 5 της απόφασης της Επιτροπής σχετικά με τους εσωτερικούς κανόνες για την εκτέλεση του τμήματος του γενικού προϋπολογισμού της Ευρωπαϊκής Ένωσης που αφορά την Επιτροπή), που τηλεφορτώνεται στο DECIDE για διυπηρεσιακή διαβούλευση.

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

| | | Έτος **2025** | Έτος **2026** | Έτος **2027** | Έτος **2028+** | Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6) | | | **ΣΥΝΟΛΟ** |
|---|---|---|---|---|---|---|---|---|---|
| ΓΔ: CONNECT | | | | | | | | | |
| ○ Ανθρώπινοι πόροι | | 0,786 | 0,786 | 0,786 | π.υ. | | | | **2,358** |
| ○ Άλλες διοικητικές δαπάνες | | 0,035 | 0,035 | 0,035 | π.υ. | | | | **0,105** |
| **ΣΥΝΟΛΟ ΓΔ CONNECT** | Πιστώσεις | **0,821** | **0,821** | **0,821** | | | | | **2,463** |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **ΣΥΝΟΛΟ πιστώσεων του ΤΟΜΕΑ 7** του πολυετούς δημοσιονομικού πλαισίου | (Σύνολο αναλήψεων υποχρεώσεων = Σύνολο πληρωμών) | **0,821** | **0,821** | **0,821** | | | | | **2,463** |

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

| | | Έτος **2025** | Έτος **2026** | Έτος **2027** | Έτος **2028+** | Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6) | | | **ΣΥΝΟΛΟ** |
|---|---|---|---|---|---|---|---|---|---|
| **ΣΥΝΟΛΟ πιστώσεωντων ΤΟΜΕΩΝ 1 έως 7** του πολυετούς δημοσιονομικού πλαισίου | Αναλήψεις υποχρεώσεων | **28,971** | **38,971** | **34,971** | **π.υ.** | | | | **102,913** |
| | Πληρωμές | **24,421** | **34,171** | **32,221** | **12,100** | | | | **102,913** |

*3.2.2. Εκτιμώμενο αποτέλεσμα που χρηματοδοτείται με επιχειρησιακές πιστώσεις*

Πιστώσεις ανάληψης υποχρεώσεων σε εκατ. EUR (με τρία δεκαδικά ψηφία)

| **Να προσδιοριστούν οι στόχοι και τα αποτελέσματα** ⇩ | | | Έτος **N** | | Έτος **N+1** | | Έτος **N+2** | | Έτος **N+3** | | Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6) | | | | | | **ΣΥΝΟΛΟ** | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **ΑΠΟΤΕΛΕΣΜΑΤΑ** | | | | | | | | | | | | | | | | | |
| | Είδος [41] | Μέσο κόστος | Αριθ. | Κόστος | Αριθ. | Κόστος | Αριθ. | Κόστος | Αριθ. | Κόστος | Αριθ. | Κόστος | Αριθ. | Κόστος | Αριθ. | Κόστος | Συνολικός αριθ. | Συνολικό κόστος |
| ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ αριθ. 1[42]… | | | | | | | | | | | | | | | | | | |
| — Αποτέλεσμα | | | | | | | | | | | | | | | | | | |
| — Αποτέλεσμα | | | | | | | | | | | | | | | | | | |
| — Αποτέλεσμα | | | | | | | | | | | | | | | | | | |
| Μερικό σύνολο για τον ειδικό στόχο αριθ. 1 | | | | | | | | | | | | | | | | | | |
| ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ αριθ. 2 ... | | | | | | | | | | | | | | | | | | |
| — Αποτέλεσμα | | | | | | | | | | | | | | | | | | |
| Μερικό σύνολο για τον ειδικό στόχο αριθ. 2 | | | | | | | | | | | | | | | | | | |
| **ΣΥΝΟΛΑ** | | | | | | | | | | | | | | | | | | |

[41] Τα αποτελέσματα είναι τα προϊόντα και οι υπηρεσίες που θα παρασχεθούν (π.χ.: αριθμός ανταλλαγών φοιτητών που θα χρηματοδοτηθούν, αριθμός χλμ. οδών που θα κατασκευαστούν κ.λπ.).

[42] Όπως περιγράφεται στο σημείο 1.4.2. «Ειδικοί στόχοι…».

*3.2.3. Συνοπτική παρουσίαση των εκτιμώμενων επιπτώσεων στις διοικητικές πιστώσεις*

– ☐ Η πρόταση/πρωτοβουλία δεν συνεπάγεται τη χρησιμοποίηση πιστώσεων διοικητικού χαρακτήρα

– ☒ Η πρόταση/πρωτοβουλία συνεπάγεται τη χρησιμοποίηση πιστώσεων διοικητικού χαρακτήρα, όπως εξηγείται κατωτέρω:

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

| | Έτος 2025 | Έτος 2026 | Έτος 2027 | Έτος N+3 | Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6) | | | **ΣΥΝΟΛΟ** |
|---|---|---|---|---|---|---|---|---|
| **ΤΟΜΕΑΣ 7 του πολυετούς δημοσιονομικού πλαισίου** | | | | | | | | |
| Ανθρώπινοι πόροι | 0,786 | 0,786 | 0,786 | | | | | **2,358** |
| Άλλες διοικητικές δαπάνες | 0,035 | 0,035 | 0,035 | | | | | **0,105** |
| **Μερικό σύνολο του ΤΟΜΕΑ 7 του πολυετούς δημοσιονομικού πλαισίου** | **0,821** | **0,821** | **0,821** | | | | | **2,463** |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Εκτός του ΤΟΜΕΑ 7[43] του πολυετούς δημοσιονομικού πλαισίου** | | | | | | | | |
| Ανθρώπινοι πόροι | | | | | | | | |
| Άλλες δαπάνεςδιοικητικού χαρακτήρα | 0,150 | 0,150 | 0,150 | | | | | **0,450** |
| **Μερικό σύνολο εκτός του ΤΟΜΕΑ 7 του πολυετούς δημοσιονομικού πλαισίου** | **0,150** | **0,150** | **0,150** | | | | | **0,450** |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **ΣΥΝΟΛΟ** | **0,971** | **0,971** | **0,971** | | | | | **2,913** |

Οι απαιτούμενες πιστώσεις για ανθρώπινους πόρους και άλλες δαπάνες διοικητικού χαρακτήρα θα καλυφθούν από τις πιστώσεις της ΓΔ που έχουν ήδη διατεθεί για τη διαχείριση της δράσης και/ή έχουν ανακατανεμηθεί στο εσωτερικό της ΓΔ και οι οποίες θα συμπληρωθούν, κατά περίπτωση, με πρόσθετα κονδύλια που ενδέχεται να χορηγηθούν στην αρμόδια για τη διαχείριση ΓΔ στο πλαίσιο της ετήσιας διαδικασίας κατανομής και λαμβανομένων υπόψη των υφιστάμενων δημοσιονομικών περιορισμών.

[43] Τεχνική και/ή διοικητική βοήθεια και δαπάνες στήριξης της εφαρμογής προγραμμάτων και/ή δράσεων της ΕΕ (πρώην γραμμές «ΒΑ»), έμμεση έρευνα, άμεση έρευνα.

3.2.3.1. Εκτιμώμενες ανάγκες σε ανθρώπινους πόρους

– ☐ Η πρόταση/πρωτοβουλία δεν συνεπάγεται τη χρησιμοποίηση ανθρώπινων πόρων

– ☒ Η πρόταση/πρωτοβουλία συνεπάγεται τη χρησιμοποίηση ανθρώπινων πόρων, όπως εξηγείται κατωτέρω:

*Εκτίμηση η οποία πρέπει να εκφράζεται σε μονάδες ισοδυνάμων πλήρους απασχόλησης*

| | Έτος **2025** | Έτος **2026** | Έτος 2027 | Έτος **N+3** | Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6) | | |
|---|---|---|---|---|---|---|---|
| **Θέσεις απασχόλησης του πίνακα προσωπικού (θέσεις μόνιμων και έκτακτων υπαλλήλων)** | | | | | | | |
| 20 01 02 01 (στην έδρα και στις αντιπροσωπείες της Επιτροπής) | 3 | 3 | 3 | | | | |
| 20 01 02 03 (αντιπροσωπείες της ΕΕ) | | | | | | | |
| 01 01 01 01 (έμμεση έρευνα) | | | | | | | |
| 01 01 01 11 (άμεση έρευνα) | | | | | | | |
| Άλλες γραμμές του προϋπολογισμού (να προσδιοριστούν) | | | | | | | |
| **Εξωτερικό προσωπικό (σε μονάδα ισοδυνάμου πλήρους απασχόλησης: ΙΠΑ)**[44] | | | | | | | |
| 20 02 01 (AC, END, INT από το συνολικό κονδύλιο) | 3 | 3 | 3 | | | | |
| 20 02 03 (AC, AL, END, INT και JPD στις αντιπροσωπείες της ΕΕ) | | | | | | | |
| **XX** 01 xx **yy zz** [45] — στην έδρα | | | | | | | |
| **XX** 01 xx **yy zz** [45] — στις αντιπροσωπείες της ΕΕ | | | | | | | |
| 01 01 01 02 (AC, END, INT — έμμεση έρευνα) | | | | | | | |
| 01 01 01 12 (AC, END, INT — άμεση έρευνα) | | | | | | | |
| Άλλες γραμμές του προϋπολογισμού (να προσδιοριστούν) | | | | | | | |
| **ΣΥΝΟΛΟ** | **6** | **6** | **6** | | | | |

**XX** είναι ο σχετικός τομέας πολιτικής ή ο σχετικός τίτλος του προϋπολογισμού.

Οι ανάγκες σε ανθρώπινους πόρους θα καλυφθούν από το προσωπικό της ΓΔ που έχει ήδη διατεθεί για τη διαχείριση της δράσης και/ή έχει ανακατανεμηθεί στο εσωτερικό της ΓΔ και το οποίο θα συμπληρωθεί, εάν χρειαστεί, από πρόσθετους πόρους που μπορεί να διατεθούν στην αρμόδια για τη διαχείριση ΓΔ στο πλαίσιο της ετήσιας διαδικασίας κατανομής και λαμβανομένων υπόψη των υφιστάμενων δημοσιονομικών περιορισμών.

Περιγραφή των προς εκτέλεση καθηκόντων:

| | |
|---|---|
| Μόνιμοι και έκτακτοι υπάλληλοι | - καθορισμός δράσεων ετοιμότητας σύμφωνα με τις εκτιμήσεις κινδύνου (άρθρο 11),<br>- εκπόνηση πιθανών εκτελεστικών πράξεων (δύο για τα SOC και δύο για τον μηχανισμό έκτακτης ανάγκης για την κυβερνοασφάλεια),<br>- διαχείριση των συμφωνιών υποδοχής και χρήσης για τα SOC,<br>- δημιουργία και διαχείριση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, απευθείας ή μέσω συμφωνίας συνεισφοράς με τον ENISA. |
| Εξωτερικό προσωπικό | Υπό την επίβλεψη υπαλλήλου |

[44] AC = Συμβασιούχος υπάλληλος· AL = Τοπικός υπάλληλος· END = Αποσπασμένος εθνικός εμπειρογνώμονας· INT = Προσωρινό προσωπικό· JPD = Νέος επαγγελματίας σε αντιπροσωπεία της ΕΕ.

[45] Επιμέρους ανώτατο όριο εξωτερικού προσωπικού που καλύπτεται από επιχειρησιακές πιστώσεις (πρώην γραμμές «ΒΑ»).

| | |
|---|---|
| | - καθορισμός δράσεων ετοιμότητας σύμφωνα με τις εκτιμήσεις κινδύνου (άρθρο 11),<br>- εκπόνηση πιθανών εκτελεστικών πράξεων (δύο για τα SOC και δύο για τον μηχανισμό έκτακτης ανάγκης για την κυβερνοασφάλεια),<br>- διαχείριση των συμφωνιών υποδοχής και χρήσης για τα SOC,<br>- δημιουργία και διαχείριση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, απευθείας ή μέσω συμφωνίας συνεισφοράς με τον ENISA. |

### 3.2.4. *Συμβατότητα με το ισχύον πολυετές δημοσιονομικό πλαίσιο*

Η πρόταση/πρωτοβουλία:

– [X] μπορεί να χρηματοδοτηθεί εξ ολοκλήρου με ανακατανομή εντός του οικείου τομέα του πολυετούς δημοσιονομικού πλαισίου (ΠΔΠ).

| Να εξηγηθεί ο απαιτούμενος αναπρογραμματισμός και να προσδιοριστούν οι σχετικές γραμμές του προϋπολογισμού και τα αντίστοιχα ποσά. Να υποβληθεί πίνακας Excel σε περίπτωση σημαντικού αναπρογραμματισμού. |
|---|

| | 2023 | 2024 | 2025 | 2026 | 2027 | σύνολο |
|---|---|---|---|---|---|---|
| SO1 | 16,232,897 | 20,528,765 | 17,406,899 | 16,223,464 | 10,022,366 | 80,414,391 |
| | | | | | | |
| αρχικό SO2 | 226,316,819 | 295,067,000 | 195,649,000 | 221,809,000 | 246,608,000 | 1,185,449,819 |
| Προς πρωτοβουλία στον ΚΥΒΕΡΝΟΧΩΡΟ | | | 18,000,000 | 28,000,000 | 19,000,000 | 65,000,000 |
| **NEO SO2** | **226,316,819** | **295,067,000** | **177,649,000** | **193,809,000** | **227,608,000** | **1,120,449,819** |
| | | | | | | |
| SO3 DB 24 | 24,361,553 | 35,596,172 | 3,638,000 | 3,638,000 | 11,175,000 | 78,408,725 |
| Από SO2-SO4 | | | 15,000,000 | 15,000,000 | 6,000,000 | 36,000,000 |
| **Νέο SO3** | **24,361,553** | **35,596,172** | **18,638,000** | **18,638,000** | **17,175,000** | **114,408,725** |
| | | | | | | |
| αρχικό ECCC | 176,222,303 | 208,374,879 | 104,228,130 | 90,704,986 | 84,851,497 | 664,381,795 |
| Από SO2-SO4 | | | 13,000,000 | 23,000,000 | 28,000,000 | 64,000,000 |
| **Νέο ECCC** | **176,222,303** | **208,374,879** | **117,228,130** | **113,704,986** | **112,851,497** | **728,381,795** |
| | | | | | | |
| αρχικό SO4 | 66,902,708 | 64,892,032 | 56,577,977 | 70,477,245 | 72,107,201 | 330,957,163 |
| Προς πρωτοβουλία στον ΚΥΒΕΡΝΟΧΩΡΟ | | | 10,000,000 | 10,000,000 | 15,000,000 | 35,000,000 |
| **NEO SO4** | **66,902,708** | **64,892,032** | **46,577,977** | **60,477,245** | **57,107,201** | **295,957,163** |

– [ ] συνεπάγεται τη χρησιμοποίηση του αδιάθετου περιθωρίου στο πλαίσιο του αντίστοιχου τομέα του ΠΔΠ και/ή τη χρήση ειδικών μηχανισμών, όπως ορίζεται στον κανονισμό για το ΠΔΠ.

| Να εξηγηθούν οι απαιτούμενες ενέργειες και να προσδιοριστούν οι σχετικοί τομείς και οι σχετικές γραμμές του προϋπολογισμού, τα αντίστοιχα ποσά και οι μηχανισμοί που προτείνεται να χρησιμοποιηθούν. |
|---|

– [ ] συνεπάγεται την αναθεώρηση του ΠΔΠ.

| Να εξηγηθούν οι απαιτούμενες ενέργειες και να προσδιοριστούν οι σχετικοί τομείς και οι σχετικές γραμμές του προϋπολογισμού, καθώς και τα αντίστοιχα ποσά. |
|---|

### 3.2.5. *Συμμετοχή τρίτων στη χρηματοδότηση*

Η πρόταση/πρωτοβουλία:

– [X] δεν προβλέπει συγχρηματοδότηση από τρίτους

– [ ] προβλέπει τη συγχρηματοδότηση από τρίτους που εκτιμάται παρακάτω:

Πιστώσεις σε εκατ. EUR (με τρία δεκαδικά ψηφία)

| | Έτος **N**[46] | Έτος **N+1** | Έτος **N+2** | Έτος **N+3** | Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6) | | | Σύνολο |
|---|---|---|---|---|---|---|---|---|
| Προσδιορισμός του φορέα συγχρηματοδότησης | | | | | | | | |
| ΣΥΝΟΛΟ συγχρηματοδοτούμενων πιστώσεων | | | | | | | | |

[46] Το έτος Ν είναι το έτος έναρξης εφαρμογής της πρότασης/πρωτοβουλίας. Να αντικατασταθεί το «Ν» με το αναμενόμενο πρώτο έτος εφαρμογής (για παράδειγμα: 2021). Το ίδιο και για τα επόμενα έτη.

### 3.3. Εκτιμώμενες επιπτώσεις στα έσοδα

– [X] Η πρόταση/πρωτοβουλία δεν έχει δημοσιονομικές επιπτώσεις στα έσοδα.

– ☐ Η πρόταση/πρωτοβουλία έχει τις δημοσιονομικές επιπτώσεις που περιγράφονται κατωτέρω:

  – ☐ στους ιδίους πόρους

  – ☐ στα λοιπά έσοδα

  – Να αναφερθεί αν τα έσοδα προορίζονται για γραμμές δαπανών ☐

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

| Γραμμή εσόδων του προϋπολογισμού: | Διαθέσιμες πιστώσεις για το τρέχον οικονομικό έτος | Επιπτώσεις της πρότασης/πρωτοβουλίας[47] | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Έτος **N** | Έτος **N+1** | Έτος **N+2** | Έτος **N+3** | Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6) | | |
| Άρθρο ……. | | | | | | | | |

Ως προς τα έσοδα «για ειδικό προορισμό», να προσδιοριστούν οι γραμμές δαπανών του προϋπολογισμού που επηρεάζονται.

[…]

Άλλες παρατηρήσεις (π.χ. μέθοδος/τύπος για τον υπολογισμό των επιπτώσεων στα έσοδα ή τυχόν άλλες πληροφορίες).

[…]

[47] Όσον αφορά τους παραδοσιακούς ιδίους πόρους (δασμούς, εισφορές ζάχαρης), τα αναγραφόμενα ποσά πρέπει να είναι καθαρά ποσά, δηλ. τα ακαθάριστα ποσά μετά την αφαίρεση του 20 % για έξοδα είσπραξης.