ΤΡΟΠΟΛΟΓΙΕΣ 001-001
κατάθεση: Επιτροπή Βιομηχανίας, Έρευνας και Ενέργειας

Έκθεση
Lina Gálvez Muñoz **A9-0426/2023**
Καθορισμός μέτρων για την ενίσχυση της αλληλεγγύης και των ικανοτήτων της Ένωσης για την ανίχνευση, την προετοιμασία και την αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας

Πρόταση κανονισμού (COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Τροπολογία 1

ΤΡΟΠΟΛΟΓΙΕΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ*

στην πρόταση της Επιτροπής

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 *και την τροποποίηση του κανονισμού (ΕΕ) 2021/694*

* Τροπολογίες: το νέο ή το τροποποιημένο κείμενο σημειώνεται με ***έντονους πλάγιους*** χαρακτήρες· οι διαγραφές σημειώνονται με το σύμβολο ▌.

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 της πληροφορίας και των επικοινωνιών και η εξάρτηση από αυτές είναι πλέον θεμελιώδεις πτυχές***, αλλά ταυτόχρονα έχουν εισαγάγει πιθανές ευπάθειες*** 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 ***τόσο σε επίπεδο Ένωσης όσο και παγκόσμια όσον αφορά τις μεθόδους και τον αντίκτυπό τους***, 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 ***για τις οικονομίες και τις δημοκρατίες*** σε κρίσιμες υποδομές σε ολόκληρη την Ένωση 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 ***και*** εγκληματικών παραγόντων ▌ 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 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. ***Απαιτείται επομένως στενή συνεργασία μεταξύ του δημόσιου τομέα, του ιδιωτικού τομέα, της πανεπιστημιακής κοινότητας και των μέσων ενημέρωσης. Επιπλέον, η αντίδραση της Ένωσης πρέπει να συντονίζεται με διεθνείς***

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

οργανισμούς, καθώς και με αξιόπιστους και ομονοούντες διεθνείς εταίρους. Αξιόπιστοι και ομονοούντες διεθνείς εταίροι είναι οι χώρες που συμμερίζονται τις αξίες της Ένωσης για δημοκρατία, προσήλωση στα ανθρώπινα δικαιώματα, ουσιαστική πολυμέρεια, και βασιζόμενη σε κανόνες τάξη, σύμφωνα με τα διεθνή πλαίσια και συμφωνίες συνεργασίας. Για να διασφαλιστούν η συνεργασία με αξιόπιστους και ομονοούντες διεθνείς εταίρους και η προστασία έναντι συστημικών αντιπάλων, οι οντότητες που είναι εγκατεστημένες σε τρίτες χώρες οι οποίες δεν είναι συμβαλλόμενα μέρη της ΣΔΣ δεν θα πρέπει να επιτρέπεται να συμμετέχουν σε δημόσιες συμβάσεις δυνάμει του παρόντος κανονισμού.

(3) Είναι αναγκαίο 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, με την ενίσχυση 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***, ιδίως των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων (ΜΜΕ), συμπεριλαμβανομένων των νεοφυών επιχειρήσεων*** και των οντοτήτων που διαχειρίζονται κρίσιμες υποδομές, ***συμπεριλαμβανομένων των τοπικών ή περιφερειακών αρχών,*** έναντι των αυξανόμενων απειλών κυβερνοασφάλειας, οι οποίες μπορούν να έχουν καταστροφικές κοινωνικές και οικονομικές επιπτώσεις. Ως εκ τούτου, απαιτούνται επενδύσεις σε υποδομές και υπηρεσίες***, καθώς και ικανότητες ανάπτυξης δεξιοτήτων κυβερνοασφάλειας*** 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.

(3α) Οι κυβερνοεπιθέσεις στοχεύουν συχνά τοπικές, περιφερειακές ή εθνικές δημόσιες υπηρεσίες και υποδομές. Οι τοπικές αρχές συγκαταλέγονται στους πλέον ευπαθείς στόχους κυβερνοεπιθέσεων λόγω της έλλειψης οικονομικών και ανθρώπινων πόρων. Είναι επομένως ιδιαίτερα σημαντικό, οι φορείς λήψης αποφάσεων σε τοπικό επίπεδο να συνειδητοποιήσουν την ανάγκη να αυξηθούν η ψηφιακή ανθεκτικότητα και η ικανότητά τους να μειώνουν τον αντίκτυπο των κυβερνοεπιθέσεων, και να αξιοποιήσουν τις ευκαιρίες που προβλέπονται στον παρόντα κανονισμό.

(4) Η Ένωση έχει ήδη λάβει σειρά μέτρων για τη μείωση των ευπαθειών και την αύξηση της ανθεκτικότητας των κρίσιμων υποδομών και οντοτήτων έναντι των κινδύνων κυβερνοασφάλειας, ιδίως με την οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού

[4] https://wayback.archive-it.org/12090/20230417171535/https://futureu.europa.eu/el/

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, 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, ▌ αντιμετώπιση ***και ανάκαμψη για*** απειλές και περιστατικά 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 την κατάσταση κυβερνοασφάλειας 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 ***δικτύου*** 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

---

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).

9 Συμπεράσματα του Συμβουλίου σχετικά με την κατάσταση κυβερνοασφάλειας της Ευρωπαϊκής Ένωσης, 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).

παρόχους και της δοκιμής κρίσιμων οντοτήτων για πιθανές ευπάθειες 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 ***πρόληψη και την*** αντιμετώπιση σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας. Ως εκ τούτου, θα πρέπει να αναπτυχθεί ***πανευρωπαϊκό δίκτυο*** SOC (ευρωπαϊκή Κυβερνοασπίδα) για την οικοδόμηση και ενίσχυση κοινών ικανοτήτων ανίχνευσης και αντίληψης της κατάστασης***, με την ενίσχυση της ικανότητας της Ένωσης για τον εντοπισμό απειλών και την ανταλλαγή πληροφοριών***· 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 ***για την κυβερνοασφάλεια*** στο πλαίσιο του ειδικού στόχου 3 του προγράμματος «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.

(9α) Υπό το φως των γεωπολιτικών εξελίξεων και του αυξανόμενου τοπίου των

[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).

κυβερνοαπειλών (EPP 52) και προκειμένου να διασφαλιστούν η συνέχεια και η περαιτέρω ανάπτυξη των μέτρων που ορίζονται στον παρόντα κανονισμό μετά το 2027, ιδίως της ευρωπαϊκής Κυβερνοασπίδας και του Μηχανισμού έκτακτης ανάγκης για την κυβερνοασφάλεια, είναι αναγκαίο να διασφαλιστεί ειδική γραμμή του προϋπολογισμού στο πολυετές δημοσιονομικό πλαίσιο για την περίοδο 2028-2034. Τα κράτη μέλη θα πρέπει επίσης να επιδιώξουν να δεσμευτούν ότι θα στηρίξουν όλα τα αναγκαία μέτρα για τη μείωση των κυβερνοαπειλών και των περιστατικών σε ολόκληρη την Ένωση, και για την ενίσχυση της αλληλεγγύης.

(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 ***κανονισμό (ΕΕ, Ευρατόμ) 2018/1046 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου***[12] 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[13].

(11) Για τους σκοπούς της χρηστής δημοσιονομικής διαχείρισης, θα πρέπει να θεσπιστούν ειδικοί κανόνες για τη μεταφορά αχρησιμοποίητων πιστώσεων αναλήψεων 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 κανονισμό ***(ΕΕ, Ευρατόμ) 2018/1046***, μεγιστοποιώντας έτσι την ικανότητα του Μηχανισμού έκτακτης ανάγκης για την κυβερνοασφάλεια να στηρίζει τα κράτη μέλη όσον αφορά την αποτελεσματική αντιμετώπιση κυβερνοαπειλών.

(11α) Ο Μηχανισμός έκτακτης ανάγκης για την κυβερνοασφάλεια και η Εφεδρεία της ΕΕ για την κυβερνοασφάλεια που θεσπίζεται με τον παρόντα κανονισμό αποτελούν νέες πρωτοβουλίες και δεν προβλέφθηκαν κατά τη θέσπιση του πολυετούς δημοσιονομικού πλαισίου για την περίοδο 2021-2027, και η χρηματοδότηση των εν λόγω πρωτοβουλιών γίνεται με γνώμονα τον περιορισμό της μείωσης της χρηματοδότησης για άλλες προτεραιότητες του προγράμματος «Ψηφιακή Ευρώπη» στον ελάχιστο δυνατό βαθμό. Επομένως, το ποσό των

---

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, την τροποποίηση των κανονισμών (ΕΕ) αριθ. 1296/2013, (ΕΕ) αριθ. 1301/2013, (ΕΕ) αριθ. 1303/2013, (ΕΕ) αριθ. 1304/2013, (ΕΕ) αριθ. 1309/2013, (ΕΕ) αριθ. 1316/2013, (ΕΕ) αριθ. 223/2014, (ΕΕ) αριθ. 283/2014 και της απόφασης αριθ. 541/2014/ΕΕ και για την κατάργηση του κανονισμού (ΕΕ, Ευρατόμ) αριθ. 966/2012 (ΕΕ L 193 της 30.7.2018, σ. 1), ELI: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32018R1046).***

13 ***Κανονισμός (ΕΕ, Ευρατόμ) 2020/2092 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Δεκεμβρίου 2020, περί γενικού καθεστώτος αιρεσιμότητας για την προστασία του προϋπολογισμού της Ένωσης, (ΕΕ L 433 I της 22.12.2020, σ. 1, ELI:). https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32020R2092).***

χρηματοδοτικών πόρων που προορίζονται για την Εφεδρεία της ΕΕ για την κυβερνοασφάλεια θα πρέπει να μειωθεί και θα πρέπει πρωτίστως να αντληθεί από τα αδιάθετα περιθώρια στο πλαίσιο των ανώτατων ορίων του πολυετούς δημοσιονομικού πλαισίου ή να κινητοποιηθεί μέσω των μη θεματικών ειδικών μέσων του πολυετούς δημοσιονομικού πλαισίου. Κάθε διάθεση ή ανακατανομή κονδυλίων από υφιστάμενα προγράμματα θα πρέπει να περιορίζεται στο απολύτως ελάχιστο, προκειμένου να προστατεύονται τα υφιστάμενα προγράμματα, ιδίως το Erasmus+, από αρνητικές επιπτώσεις και να διασφαλίζεται ότι τα εν λόγω προγράμματα μπορούν να επιτύχουν τους στόχους που έχουν τεθεί.

(12) Για την αποτελεσματικότερη πρόληψη, αξιολόγηση***,*** αντιμετώπιση ***και ανάκαμψη*** σε σχέση με κυβερνοαπειλές και περιστατικά, 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. ***Μια προορατική προσέγγιση για τον εντοπισμό, τον μετριασμό και την πρόληψη πιθανών κυβερνοαπειλών περιλαμβάνει αυξημένη ικανότητα προηγμένων ικανοτήτων ανίχνευσης που είναι αναγκαίες για την εξάλειψη προηγμένων διαρκών απειλών. Πληροφορίες σχετικά με απειλές είναι τα στοιχεία που συλλέγονται, αναλύονται και ερμηνεύονται για την κατανόηση πιθανών απειλών και κινδύνων. Με την ανάλυση και συσχέτιση τεράστιων όγκων δεδομένων, καθιστούν εμφανή σχήματα, τάσεις και δείκτες απειλής που μπορούν να αποκαλύψουν κακόβουλες δραστηριότητες ή ευπάθειες.*** Θα πρέπει να αναπτυχθεί ***ένα δίκτυο*** SOC (στο εξής: ευρωπαϊκή Κυβερνοασπίδα), που θα αποτελείται από διάφορες διαλειτουργικές διασυνοριακές πλατφόρμες, καθεμία από τις οποίες θα συγκεντρώνει διάφορα εθνικά SOC. Η εν λόγω υποδομή θα πρέπει να εξυπηρετεί 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. ***Τα εθνικά SOC είναι κεντρικές ικανότητες υπεύθυνες για τη συνεχή συλλογή πληροφοριών για απειλές και για τη βελτίωση της αντίληψης κυβερνοασφάλειας σε οντότητες υπό εθνική δικαιοδοσία μέσω της πρόληψης, της ανίχνευσης και της ανάλυσης απειλών κυβερνοασφάλειας.*** 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[14].

(13) ***Προκειμένου να συμμετάσχει στην ευρωπαϊκή Κυβερνοασπίδα,*** 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

[14] 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).

μέλος. ***Τα κράτη μέλη ενθαρρύνονται να ενσωματώσουν την εθνική ικανότητα SOC στην υφιστάμενη δομή και διακυβέρνηση στον κυβερνοχώρο, προκειμένου να αποφευχθεί η δημιουργία πρόσθετων επιπέδων διακυβέρνησης και να ευθυγραμμιστεί ο παρών κανονισμός με την ισχύουσα νομοθεσία, συμπεριλαμβανομένης της οδηγίας (ΕΕ) 2022/2555.*** Τα εν λόγω εθνικά SOC θα πρέπει να λειτουργούν ως σημείο αναφοράς και πύλη σε εθνικό επίπεδο για τη συμμετοχή ***ιδιωτικών και δημόσιων οντοτήτων, ιδίως των εθνικών SOC τους***, 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. ***Τα εθνικά SOC θα πρέπει να ενισχύσουν τη συνεργασία και την ανταλλαγή πληροφοριών μεταξύ δημόσιων και ιδιωτικών οντοτήτων, ώστε να σπάσουν τα στεγανά που υπάρχουν επί του παρόντος στην επικοινωνία. Με αυτόν τον τρόπο, μπορούν να στηρίξουν τη δημιουργία μοντέλων ανταλλαγής δεδομένων και θα πρέπει να διευκολύνουν και να ενθαρρύνουν την ανταλλαγή πληροφοριών σε ένα αξιόπιστο και ασφαλές περιβάλλον. Η στενή και συντονισμένη συνεργασία μεταξύ δημόσιων και ιδιωτικών οντοτήτων είναι πολύ σημαντική για την ενίσχυση της ανθεκτικότητας της Ένωσης στον τομέα της κυβερνοασφάλειας.***

(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, συμπεριλαμβανομένων της συλλογής και της ανταλλαγής δεδομένων και πληροφοριών σχετικά με πιθανή κακόβουλη δικτυοπαραβίαση, νέες κακόβουλες απειλές και εκμετάλλευση ευπαθειών που δεν έχουν ακόμη κλιμακωθεί σε κυβερνοπεριστατικά, και προσπάθειες ανάλυσης, 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 ***και ασφαλές*** περιβάλλον***, με την υποστήριξη του ENISA, για τη στήριξη της επιχειρησιακής συνεργασίας μεταξύ των κρατών μελών.*** Τα διασυνοριακά SOC θα πρέπει ***να διευκολύνουν και να ενθαρρύνουν την ανταλλαγή πληροφοριών σε αξιόπιστο και ασφαλές περιβάλλον και*** 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 ***ενσωματωμένη στην υφιστάμενη υποδομή κυβερνοασφάλειας, ιδίως*** στο δίκτυο CSIRT, συγκεντρώνοντας και ανταλλάσσοντας δεδομένα σχετικά με απειλές

κυβερνοασφάλειας από δημόσιες και ιδιωτικές οντότητες, ***ιδίως από τα SOC τους***, ενισχύοντας την αξία των εν λόγω δεδομένων μέσω αναλύσεων εμπειρογνωμόνων και από κοινού αποκτηθεισών υποδομών και εργαλείων αιχμής και συμβάλλοντας ***στην τεχνολογική κυριαρχία της Ένωσης, την ανοικτή στρατηγική αυτονομία, την ανταγωνιστικότητα και την ανθεκτικότητά της και στην ανάπτυξη ενός σημαντικού οικοσυστήματος κυβερνοασφάλειας, μεταξύ άλλων σε συνεργασία με αξιόπιστους και ομόφρονες διεθνείς εταίρους.***

(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 ανάγκης σε υπολογιστές (στο εξής: CERT), CSIRT, κέντρα ανταλλαγής και ανάλυσης πληροφοριών (στο εξής: ISAC), φορείς εκμετάλλευσης κρίσιμων υποδομών)***, διευκολύνοντας την υπέρβαση των στεγανών που υπάρχουν επί του παρόντος στην επικοινωνία***. ***Με τον τρόπο αυτό, τα διασυνοριακά SOC θα μπορούσαν επίσης να στηρίξουν τη δημιουργία μοντέλων ανταλλαγής δεδομένων σε ολόκληρη την Ένωση.*** Οι πληροφορίες που ανταλλάσσονται μεταξύ των συμμετεχόντων σε ένα διασυνοριακό SOC θα μπορούσαν να περιλαμβάνουν δεδομένα από δίκτυα και αισθητήρες, ροές πληροφοριών σχετικά με απειλές, ενδείξεις παραβίασης και πληροφορίες σχετικά με περιστατικά, απειλές και ευπάθειες***, συμπεριλαμβανομένων της συλλογής και της ανταλλαγής δεδομένων και πληροφοριών σχετικά με πιθανή κακόβουλη δικτυοπαραβίαση, νέες κακόβουλες απειλές και εκμετάλλευση ευπαθειών που δεν έχουν ακόμη κλιμακωθεί σε κυβερνοπεριστατικά, όπως επίσης προσπάθειες ανάλυσης***. 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[15], 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 ***του***

15 ***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) (***ΕΕ L 347 της 20.12.2013, σ. 924, ***ELI:***). https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32013D1313***).***

Συμβουλίου[16]. 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, σύμφωνα με ***την οδηγία (ΕΕ) 2022/2555***. 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 λαμβάνονται 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 ***και ασφαλές*** περιβάλλον, οι οντότητες που συμμετέχουν στην ευρωπαϊκή Κυβερνοασπίδα θα πρέπει να είναι εφοδιασμένες με προηγμένα και υψηλής ασφάλειας εργαλεία, εξοπλισμό και υποδομές ***και ειδικευμένο προσωπικό.*** 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***, τη στρατηγική αυτονομία, την ανταγωνιστικότητα και την ανθεκτικότητά της, καθώς και ένα σημαντικό οικοσύστημα κυβερνοασφάλειας***. Η συγκέντρωση επιμελημένων δεδομένων υψηλής ποιότητας θα πρέπει επίσης να συμβάλει στην ανάπτυξη προηγμένων τεχνολογιών τεχνητής νοημοσύνης και ανάλυσης δεδομένων. ***Η τεχνητή νοημοσύνη είναι πιο αποτελεσματική όταν συνδυάζεται με ανθρώπινη ανάλυση. Συνεπώς, η ύπαρξη ειδικευμένου εργατικού δυναμικό παραμένει ουσιαστική για τη συγκέντρωση δεδομένων υψηλής ποιότητας.*** Η εν λόγω συγκέντρωση θα πρέπει να διευκολυνθεί μέσω της σύνδεσης της ευρωπαϊκής

16 ***Εκτελεστική απόφαση (ΕΕ) 2018/1993 του Συμβουλίου, της 11ης Δεκεμβρίου 2018, ως προς τις ρυθμίσεις για την ολοκληρωμένη αντιμετώπιση πολιτικών κρίσεων της ΕΕ (*****ΕΕ L 320 της 17.12.2018, σ. 28,*** ***ELI: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32018D1993).***

Κυβερνοασπίδας με την πανευρωπαϊκή υποδομή υπολογιστικής υψηλών επιδόσεων που θεσπίστηκε με τον κανονισμό (ΕΕ) 2021/1173 του Συμβουλίου[17].

(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 Ύπατο Εκπρόσωπο της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας (στο εξής: Ύπατος Εκπρόσωπος), θα πρέπει σταδιακά να αναπτύξουν ειδικά πρωτόκολλα ***όρων πρόσβασης και εγγυήσεων και*** πρότυπα που θα επιτρέπουν τη συνεργασία με την κοινότητα κυβερνοάμυνας, συμπεριλαμβανομένων των όρων ελέγχου και ασφάλειας***, σεβόμενα τον μη στρατιωτικό χαρακτήρα των οργάνων και τον προορισμό της χρηματοδότησης με επακόλουθη χρήση των κονδυλίων που είναι διαθέσιμα στην κοινότητα άμυνας***. 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 Ύπατο Εκπρόσωπο ***και με πλήρη σεβασμό των δικαιωμάτων και των ελευθεριών***.

(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 ***ενωσιακού*** ή ***εθνικού δικαίου*** 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.

(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

[17] 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, ***ELI: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32021R1173***).

της άμεσης ανάκαμψης βασικών υπηρεσιών. Το μέσο αυτό θα πρέπει να επιτρέπει την ταχεία ***και ουσιαστική*** 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 ***για την κυβερνοασφάλεια*** 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 ***για την κυβερνοασφάλεια*** 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[18] 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[19], τον IPCR[20], 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 κυβερνοδιπλωματία, 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***, του ENISA*** και του επηρεαζόμενου κράτους μέλους. Όταν ζητεί στήριξη στο πλαίσιο του Μηχανισμού έκτακτης ανάγκης ***για την κυβερνοασφάλεια***, το κράτος μέλος θα πρέπει να παρέχει σχετικές πληροφορίες που αιτιολογούν την ανάγκη στήριξης.

---

18 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.

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).

20 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.

(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 ***για την κυβερνοασφάλεια*** 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 την κατάσταση κυβερνοασφάλειας της Ευρωπαϊκής Ένωσης που διενεργούν η Επιτροπή, ο Ύπατος 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[21]. 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 ***για την κυβερνοασφάλεια*** 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 ***για την κυβερνοασφάλεια*** 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 ***για την κυβερνοασφάλεια*** 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, ***ενισχύοντας ταυτόχρονα την ανθεκτικότητα της Ένωσης, συμπεριλαμβανομένης της συμμετοχής ευρωπαϊκών παρόχων υπηρεσιών διαχείρισης ασφάλειας σε κλίμακα ΜΜΕ, και διασφαλίζοντας τη δημιουργία ενός οικοσυστήματος κυβερνοασφάλειας, ιδίως μικροεπιχειρήσεων, ΜΜΕ συμπεριλαμβανομένων νεοφυών επιχειρήσεων, με επενδύσεις στην έρευνα και την καινοτομία (R&I) για την ανάπτυξη τεχνολογιών αιχμής, όπως αυτές που σχετίζονται με το υπολογιστικό νέφος και την τεχνητή νοημοσύνη. Αξιόπιστοι πάροχοι, συμπεριλαμβανομένων ΜΜΕ, θα πρέπει να μπορούν να συνεργάζονται μεταξύ τους για την εκπλήρωση των ανωτέρω κριτηρίων.*** Οι υπηρεσίες από την Εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας θα πρέπει να χρησιμοποιούνται

[21] 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.

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. ***Επομένως, η Εφεδρεία στον τομέα της κυβερνοασφάλειας θα πρέπει να παρέχει κίνητρα για την επένδυση στην έρευνα και καινοτομία, ώστε να ενισχυθεί η ανάπτυξη των τεχνολογιών αυτών. Κατά περίπτωση, θα μπορούσαν να λάβουν χώρα κοινές ασκήσεις με τους αξιόπιστους παρόχους και τους πιθανούς χρήστες της Εφεδρείας στον τομέα της κυβερνοασφάλειας, προκειμένου να διασφαλιστεί ότι η Εφεδρεία θα λειτουργεί αποτελεσματικά όταν παρουσιάζεται ανάγκη.*** 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 κυβερνοασφάλειας μπορούν επίσης να χρησιμεύσουν για τη στήριξη των θεσμικών και λοιπών οργάνων, ***υπηρεσιών*** και οργανισμών της Ένωσης, υπό παρόμοιες συνθήκες. ***Η Επιτροπή θα πρέπει να διασφαλίσει τη συμμετοχή των κρατών μελών και εκτεταμένες ανταλλαγές με τα κράτη μέλη, για την αποφυγή επικαλύψεων με παρόμοιες πρωτοβουλίες, μεταξύ άλλων στο πλαίσιο του Οργανισμού Βορειοατλαντικού Συμφώνου (ΝΑΤΟ).***

(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.***Θα πρέπει να ενθαρρυνθεί η συμμετοχή μικρότερων παρόχων δραστηριοποιούμενων σε περιφερειακό και τοπικό επίπεδο.***

(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 υπηρεσίες διαχείρισης ασφαλείας στους τομείς που καλύπτονται από τον Μηχανισμό έκτακτης ανάγκης για την ***κυβερνοασφάλεια***. ***Για την εκπλήρωση των πρόσθετων καθηκόντων που απορρέουν από την παρούσα διάταξη, ο ENISA θα πρέπει να λάβει επαρκή πρόσθετη χρηματοδότηση.***

(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, ευπάθειες 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***, υπηρεσιών*** 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 Ύπατο 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».

(37α) Οι τρίτες χώρες θα μπορούσαν να έχουν πρόσβαση σε πόρους και στήριξη σύμφωνα με τον παρόντα κανονισμό, χρησιμοποιώντας τη στήριξη για την αντιμετώπιση συμβάντων από την Εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας. Επιπλέον, ενδέχεται να χρειαστούν πάροχοι υπηρεσιών αντιμετώπισης συμβάντων από τρίτες χώρες, συμπεριλαμβανομένων τρίτων χωρών συνδεδεμένων με το πρόγραμμα «Ψηφιακή Ευρώπη» ή άλλων διεθνών χωρών-εταίρων, και μελών του ΝΑΤΟ, για την παροχή συγκεκριμένων υπηρεσιών στην Εφεδρεία της ΕΕ για την κυβερνοασφάλεια. Κατά παρέκκλιση από τον κανονισμό (ΕΕ, Ευρατόμ) 2018/1046, για να ενισχυθούν η τεχνολογική κυριαρχία της Ένωσης, η ανοικτή στρατηγική αυτονομία, η ανταγωνιστικότητα και η ανθεκτικότητά της, και να διασφαλιστούν οι στρατηγικοί πόροι, τα συμφέροντα ή η ασφάλεια της Ένωσης, δεν θα πρέπει να επιτρέπεται η συμμετοχή οντοτήτων εγκατεστημένων σε τρίτες χώρες που δεν είναι συμβαλλόμενα μέρη της ΣΔΣ και δεν έχουν υποβληθεί σε έλεγχο κατά την έννοια του κανονισμού (ΕΕ) 2019/452 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[22] και, κατά περίπτωση, σε μέτρα

[22] Κανονισμός (ΕΕ) 2019/452 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 19ης Μαρτίου 2019, για τη θέσπιση πλαισίου για τον έλεγχο των άμεσων ξένων

μετριασμού, λαμβανομένων υπόψη των στόχων που ορίζονται στον παρόντα κανονισμό. Η εξωτερική διάσταση του παρόντος κανονισμού θα πρέπει να συνάδει με τις διατάξεις που θεσπίζονται στη συμφωνία σύνδεσης στο πλαίσιο του προγράμματος «Ψηφιακή Ευρώπη». Η συμμετοχή τρίτων χωρών θα πρέπει να υπόκειται σε δημόσιο έλεγχο, με τη συμμετοχή των νομοθετικών εξουσιών, ώστε να διασφαλίζεται ότι οι πολίτες μπορούν να συμμετέχουν στη διαδικασία.

(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[23].

(38α) Είναι επιτακτικά αναγκαία η διαθεσιμότητα προσωπικού υψηλής ειδίκευσης το οποίο να μπορεί να παρέχει αξιόπιστα τις σχετικές υπηρεσίες κυβερνοασφάλειας σύμφωνα με τα υψηλότερα πρότυπα, για την αποτελεσματική υλοποίηση της ευρωπαϊκής Κυβερνοασπίδας και του Μηχανισμού έκτακτης ανάγκης για την κυβερνοασφάλεια. Είναι, συνεπώς, ανησυχητικό το γεγονός ότι η Ένωση αντιμετωπίζει έλλειψη ταλέντων, η οποία χαρακτηρίζεται από έλλειψη εξειδικευμένων επαγγελματιών, ενώ αντιμετωπίζει ένα ραγδαία εξελισσόμενο τοπίο απειλών, όπως αναγνωρίζεται στην ανακοίνωση της Επιτροπής, της 18ης Απριλίου 2023, για την Ακαδημία Δεξιοτήτων Κυβερνοασφάλειας. Είναι σημαντικό να καλυφθεί η εν λόγω έλλειψη ταλέντων μέσω της ενίσχυσης της συνεργασίας και του συντονισμού μεταξύ των διαφορετικών ενδιαφερόμενων μερών, συμπεριλαμβανομένων του ιδιωτικού τομέα, του ακαδημαϊκού τομέα, των κρατών μελών, της Επιτροπής και του ENISA, για την αναβάθμιση και τη δημιουργία συνεργειών, , ιδίως από τα SOC τους, σε όλα τα πεδία, για την επένδυση στην εκπαίδευση και στην κατάρτιση, για την ανάπτυξη εταιρικών σχέσεων μεταξύ δημόσιου και ιδιωτικού τομέα, τη στήριξη πρωτοβουλιών έρευνας και καινοτομίας, την ανάπτυξη και την από κοινού αναγνώριση κοινών προτύπων και πιστοποίησης δεξιοτήτων κυβερνοασφάλειας, μεταξύ άλλων μέσω του ευρωπαϊκού πλαισίου δεξιοτήτων κυβερνοασφάλειας. Αυτό αναμένεται επίσης να διευκολύνει την κινητικότητα των επαγγελματιών στον τομέα της κυβερνοασφάλειας εντός της Ένωσης. Ο παρών κανονισμός θα πρέπει να έχει ως

επενδύσεων στην Ένωση (ΕΕ L 79 I της 21.3.2019, σ. 1). ELI: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32019R0452.

[23] ***Κανονισμός (ΕΕ) αριθ. 182/2011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Φεβρουαρίου 2011, για τη θέσπιση κανόνων και γενικών αρχών σχετικά με τους τρόπους ελέγχου από τα κράτη μέλη της άσκησης των εκτελεστικών αρμοδιοτήτων από την Επιτροπή (ΕΕ L 55 της 28.2.2011, σ. 13, ELI: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32011R0182).***

στόχο την προώθηση ενός πιο ποικιλόμορφου εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας. Όλα τα μέτρα που αποσκοπούν στην αύξηση των δεξιοτήτων κυβερνοασφάλειας απαιτούν δικλίδες για την αποφυγή της διαρροής επιστημονικού δυναμικού και του κινδύνου για την κινητικότητα του εργατικού δυναμικού.

(38β) Απαιτείται ενίσχυση των εξειδικευμένων, διεπιστημονικών και γενικών δεξιοτήτων και ικανοτήτων σε ολόκληρη την Ένωση, με ιδιαίτερη έμφαση στις γυναίκες, καθώς το χάσμα μεταξύ των φύλων εξακολουθεί να υφίσταται στον τομέα της κυβερνοασφάλειας, όπου η μέση παρουσία των γυναικών ανέρχεται σε 20% παγκοσμίως. Οι γυναίκες πρέπει να είναι παρούσες και να αποτελούν μέρος του σχεδιασμού του ψηφιακού μέλλοντος και της διακυβέρνησής του.

(38γ) Η ενίσχυση της έρευνας και της καινοτομίας (R&I) στον τομέα της κυβερνοασφάλειας αποσκοπεί στην αύξηση της ανθεκτικότητας και της ανοικτής στρατηγικής αυτονομίας της Ένωσης. Ομοίως, είναι σημαντικό να δημιουργηθούν συνέργειες με προγράμματα R&I και με υφιστάμενα μέσα και θεσμικά όργανα και να ενισχυθούν η συνεργασία και ο συντονισμός μεταξύ των διαφόρων ενδιαφερόμενων μερών, συμπεριλαμβανομένων του ιδιωτικού τομέα, της κοινωνίας των πολιτών, της ακαδημαϊκής κοινότητας, των κρατών μελών, της Επιτροπής και του ENISA·

(38δ) Ο παρών κανονισμός θα συμβάλει στη δέσμευση της ευρωπαϊκής διακήρυξης σχετικά με τα ψηφιακά δικαιώματα και τις ψηφιακές αρχές για την ψηφιακή δεκαετία, που συνδέεται με την προστασία των συμφερόντων των δημοκρατιών, των πολιτών, των επιχειρήσεων και των δημόσιων οργανισμών μας από τους κινδύνους κυβερνοασφάλειας και το κυβερνοέγκλημα, συμπεριλαμβανομένων των παραβιάσεων δεδομένων και της κλοπής ή χειραγώγησης ταυτότητας. Η εφαρμογή του παρόντος κανονισμού θα συμβάλει επίσης στη βελτίωση της εφαρμογής άλλων νομοθετικών πράξεων, για παράδειγμα σχετικά με την τεχνητή νοημοσύνη, την προστασία της ιδιωτικότητας των δεδομένων και τη ρύθμιση των δεδομένων όσον αφορά την κυβερνοασφάλεια και την κυβερνοανθεκτικότητα.

(38ε) Η ενίσχυση μιας αντίληψης κυβερνοασφάλειας στην οποία η ασφάλεια, συμπεριλαμβανομένης της ασφάλειας του ψηφιακού περιβάλλοντος, θεωρείται δημόσιο αγαθό, θα έχει καθοριστική σημασία για την επιτυχή εφαρμογή του παρόντος κανονισμού. Συνεπώς, η ανάπτυξη μέτρων για τη συμπερίληψη και την αύξηση της ευαισθητοποίησης των πολιτών θα πρέπει να αποτελέσει ένα ακόμη μέσο για τη διασφάλιση της διαφύλαξης των δημοκρατιών και των θεμελιωδών αξιών μας.

(38στ) Προκειμένου να συμπληρωθούν ορισμένα μη ουσιώδη στοιχεία του παρόντος κανονισμού, θα πρέπει να ανατεθεί στην Επιτροπή η εξουσία έκδοσης πράξεων σύμφωνα με το άρθρο 290 ΣΛΕΕ, προκειμένου να καθοριστούν οι προϋποθέσεις διαλειτουργικότητας μεταξύ των διασυνοριακών SOC, να καθοριστούν οι διαδικαστικές ρυθμίσεις για την ανταλλαγή πληροφοριών μεταξύ των διασυνοριακών SOC, αφενός, και του EU-CyCLONe, του δικτύου CSIRT και της Επιτροπής, αφετέρου, να προσδιοριστούν οι τύποι και ο αριθμός των υπηρεσιών αντιμετώπισης που απαιτούνται για την Εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας και να προσδιοριστούν περαιτέρω οι λεπτομερείς ρυθμίσεις για την κατανομή των υπηρεσιών στήριξης της Εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. Είναι ιδιαίτερα σημαντικό να διεξάγει η Επιτροπή κατάλληλες

διαβουλεύσεις κατά τη διάρκεια των προπαρασκευαστικών εργασιών της, μεταξύ άλλων σε επίπεδο ειδικών, και οι διαβουλεύσεις αυτές να διεξάγονται σύμφωνα με τις αρχές που ορίζονται στη διοργανική συμφωνία της 13ης Απριλίου 2016 για τη βελτίωση του νομοθετικού έργου[24]. Πιο συγκεκριμένα, προκειμένου να διασφαλιστεί η ίση συμμετοχή στην προετοιμασία των κατ' εξουσιοδότηση πράξεων, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο λαμβάνουν όλα τα έγγραφα κατά τον ίδιο χρόνο με τους ειδικούς των κρατών μελών, και οι ειδικοί τους έχουν συστηματικά πρόσβαση στις συνεδριάσεις των ομάδων ειδικών της Επιτροπής που ασχολούνται με την προετοιμασία κατ' εξουσιοδότηση πράξεων.

(39) ***Οι στόχοι του παρόντος κανονισμού, δηλαδή η ενίσχυση των ικανοτήτων της Ένωσης όσον αφορά την πρόληψη, τον εντοπισμό, την αντιμετώπιση και την εξουδετέρωση των κυβερνοαπειλών, και η θέσπιση γενικού πλαισίου για την άρση των στεγανών στην επικοινωνία δεν μπορούν να επιτευχθούν επαρκώς από τα κράτη μέλη, μπορούν όμως να επιτευχθούν*** καλύτερα σε επίπεδο Ένωσης. 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. ***Σύμφωνα με την αρχή της αναλογικότητας, όπως διατυπώνεται στο εν λόγω άρθρο, ο παρών*** κανονισμός δεν υπερβαίνει τα αναγκαία 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 πανευρωπαϊκού ***δικτύου*** 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) ενίσχυση της κοινής ανίχνευσης και επίγνωσης σε επίπεδο Ένωσης της κατάστασης σε σχέση με κυβερνοαπειλές και συμβάντα, που επιτρέπει ***τη στήριξη της βιομηχανικής***

---

[24] ***ΕΕ L 123 της 12.5.2016, σ. 1, ELI: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016Q0512(01).***

ικανότητας της Ένωσης και των κρατών μελών στον τομέα της κυβερνοασφάλειας, και ενίσχυση της ανταγωνιστικής θέσης της βιομηχανίας, ***ιδίως των πολύ μικρών επιχειρήσεων, των ΜΜΕ, συμπεριλαμβανομένων των νεοφυών επιχειρήσεων***, και των τομέων υπηρεσιών στην Ένωση σε ολόκληρη την ψηφιακή οικονομία, και συμβολή στην τεχνολογική κυριαρχία της Ένωσης στην ανοικτή στρατηγική αυτονομία***, ανταγωνιστικότητα και ανθεκτικότητα στον εν λόγω τομέα, με την ενίσχυση του οικοσυστήματος κυβερνοασφάλειας με σκοπό τη διασφάλιση ισχυρών ικανοτήτων της Ένωσης, μεταξύ άλλων σε συνεργασία με διεθνείς εταίρους***·

β) αύξηση του βαθμού ετοιμότητας των οντοτήτων που δραστηριοποιούνται σε τομείς κρίσιμης και εξαιρετικά κρίσιμης σημασίας σε ολόκληρη την Ένωση και 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) 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.

γα) ανάπτυξη, με συντονισμένο τρόπο, δεξιοτήτων, τεχνογνωσίας και ικανοτήτων του εργατικού δυναμικού, με σκοπό την προστασία της κυβερνοασφάλειας και τη δημιουργία συνεργειών με την Ακαδημία Δεξιοτήτων Κυβερνοασφάλειας.

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:

(-1α) «Εθνικό κέντρο επιχειρήσεων ασφάλειας» ή «εθνικό SOC»: κεντρική εθνική ικανότητα συνεχούς συλλογής και ανάλυσης πληροφοριών σχετικά με κυβερνοαπειλές και βελτίωσης της ικανότητας κυβερνοασφάλειας σύμφωνα με το άρθρο 4·

(1) ***«Διασυνοριακό κέντρο επιχειρήσεων ασφάλειας» ή «διασυνοριακό SOC»:*** πολυκρατική πλατφόρμα που συγκεντρώνει σε μια συντονισμένη δομή δικτύου τα εθνικά SOC ***σύμφωνα με το άρθρο 5***·

(2) ***«δημόσιος φορέας»***: ***φορείς*** δημοσίου δικαίου, όπως ορίζεται στο άρθρο 2 παράγραφος 1 σημείο 4) της οδηγίας 2014/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[25]·

(3) ***«κοινοπραξία υποδοχής»***: κοινοπραξία αποτελούμενη από συμμετέχοντα κράτη, εκπροσωπούμενα από εθνικά SOC***, σύμφωνα με το άρθρο 5***.·

[25] 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).

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

(4α) «κρίσιμη οντότητα»: κρίσιμη οντότητα όπως ορίζεται στο άρθρο 2 σημείο 1) της οδηγίας (ΕΕ) 2022/2557 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[26]·

(5) ***«οντότητες που δραστηριοποιούνται σε τομείς κρίσιμης και εξαιρετικά κρίσιμης σημασίας»:*** οντότητες ***στους τομείς*** που απαριθμούνται στα ***παραρτήματα*** I και II της οδηγίας (ΕΕ) 2022/2555·

(5α) «χειρισμός περιστατικών»: ο χειρισμός περιστατικών όπως ορίζεται στο άρθρο 6 σημείο 8) της οδηγίας (ΕΕ) 2022/2555·

(5β) «κίνδυνος»: κίνδυνος όπως ορίζεται στο άρθρο 6 σημείο 9 της οδηγίας (ΕΕ) 2022/2555·

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

(6α) «σημαντική κυβερνοαπειλή»: σημαντική κυβερνοαπειλή όπως ορίζεται στο άρθρο 6 σημείο 11) της οδηγίας (ΕΕ) 2022/2555·

(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) ***«αντίδραση»***: 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·

(10α) «πάροχος υπηρεσιών διαχείρισης ασφάλειας»: πάροχος υπηρεσιών διαχείρισης κινδύνων κυβερνοασφάλειας όπως ορίζεται στο άρθρο 6 σημείο 40) της οδηγίας (ΕΕ) 2022/2555·

(11) ***«αξιόπιστοι πάροχοι υπηρεσιών διαχείρισης ασφάλειας»***: πάροχοι υπηρεσιών διαχείρισης κινδύνων κυβερνοασφάλειας οι οποίοι επιλέγονται ***ώστε να συμπεριληφθούν στην Εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας*** σύμφωνα με το άρθρο 16 του παρόντος κανονισμού.

---

[26] Οδηγία (ΕΕ) 2022/2557 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, για την ανθεκτικότητα των κρίσιμων οντοτήτων και την κατάργηση της οδηγίας 2008/114/ΕΚ του Συμβουλίου (ΕΕ L 333 της 27.12.2022, σ. 164, ELI: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32022L2557).

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 την πρόληψη περιστατικών 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 ανταλλάσσει δεδομένα σχετικά με κυβερνοαπειλές και περιστατικά από διάφορες πηγές μέσω διασυνοριακών SOC ***και, κατά περίπτωση, έχει ανταλλαγή πληροφοριών με το δίκτυο CSIRT***·

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***,*** ***μεταξύ άλλων μέσω της παροχής συγκεκριμένων συστάσεων σε οντότητες***,

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 είναι ***σε θέση να συμμετέχει*** στην ευρωπαϊκή Κυβερνοασπίδα, κάθε κράτος μέλος ορίζει τουλάχιστον ένα εθνικό SOC. Το εθνικό SOC ***αποτελεί κεντρική ικανότητα σε δημόσιο φορέα***. ***Όταν είναι δυνατόν, τα εθνικά SOC ενσωματώνονται στις CSIRT ή σε άλλες υφιστάμενες υποδομές και διακυβέρνηση κυβερνοασφάλειας.***

Έχει την ικανότητα να ενεργεί ως σημείο αναφοράς και πύλη προς άλλους δημόσιους και ιδιωτικούς οργανισμούς σε εθνικό επίπεδο, ***ιδίως τα εθνικά SOC τους***, για τη συλλογή και την ανάλυση πληροφοριών σχετικά με απειλές και περιστατικά κυβερνοασφάλειας ***και, κατά περίπτωση, για την ανταλλαγή των εν λόγω πληροφοριών με μέλη του δικτύου CSIRT του εν λόγω κράτους μέλους,*** καθώς και για τη συμβολή σε διασυνοριακό SOC. Είναι

εφοδιασμένο με προηγμένες τεχνολογίες ***πρόληψης,*** ανίχνευσης, συγκέντρωσης και ανάλυσης δεδομένων σχετικών με απειλές και περιστατικά κυβερνοασφάλειας.

Ένα εθνικό SOC ή CSIRT μπορεί να ζητήσει τηλεμετρία, αισθητήρα ή δεδομένα καταγραφής των εθνικών κρίσιμων οντοτήτων του από παρόχους υπηρεσιών διαχείρισης ασφάλειας που παρέχουν υπηρεσία στην κρίσιμη οντότητα. Τα εν λόγω δεδομένα ανταλλάσσονται σύμφωνα με το ενωσιακό δίκαιο για την προστασία των δεδομένων και με μοναδικό σκοπό την υποστήριξη του εθνικού SOC ή της CSIRT στον εντοπισμό και την πρόληψη απειλών και περιστατικών κυβερνοασφάλειας.

2. Κατόπιν πρόσκλησης εκδήλωσης ενδιαφέροντος, τα εθνικά SOC ***μπορούν να*** 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. ***Ένα διασυνοριακό SOC σχεδιάζεται για τον εντοπισμό και την ανάλυση κυβερνοαπειλών, την πρόληψη περιστατικών και τη στήριξη της παραγωγής πληροφοριών υψηλής ποιότητας, ιδίως μέσω της ανταλλαγής δεδομένων από διάφορες πηγές, δημόσιες και ιδιωτικές, καθώς και μέσω της ανταλλαγής εργαλείων αιχμής και μέσω της από κοινού ανάπτυξης ικανοτήτων ανίχνευσης, ανάλυσης, πρόληψης και προστασίας στον κυβερνοχώρο σε ένα αξιόπιστο και ασφαλές περιβάλλον.***

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.

2α. Κατά παρέκκλιση από το άρθρο 176 του κανονισμού (ΕΕ, Ευρατόμ) 2018/1046, οντότητες εγκατεστημένες σε τρίτες χώρες που δεν είναι συμβαλλόμενα μέρη της ΣΔΣ δεν συμμετέχουν στην κοινή προμήθεια εργαλείων και 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, ευπάθειες, 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) ***βελτιώνει την ανταλλαγή πληροφοριών σχετικά με κυβερνοαπειλές μεταξύ εθνικών και διασυνοριακών SOC και κλαδικών ISAC με στόχο την πρόληψη, τον εντοπισμό ή τον μετριασμό των απειλών·***

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 ευπαθειών, 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 σημαντικών ▌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 ***και με ISAC της βιομηχανίας***, τα διασυνοριακά SOC εξασφαλίζουν υψηλό επίπεδο διαλειτουργικότητας μεταξύ τους ***και, όπου είναι δυνατόν, με βιομηχανικά ISAC***. Για τη διευκόλυνση της διαλειτουργικότητας μεταξύ των διασυνοριακών SOC ***και με ISAC της βιομηχανίας, τα πρότυπα και τα πρωτόκολλα ανταλλαγής πληροφοριών μπορούν να εναρμονίζονται με διεθνή πρότυπα και βέλτιστες πρακτικές της βιομηχανίας***.

Ενθαρρύνεται επίσης η κοινή προμήθεια υποδομών, υπηρεσιών και εργαλείων κυβερνοχώρου. Επιπλέον, μετά από διαβούλευση με το ECCC και τον ENISA, η Επιτροπή εξουσιοδοτείται, έως ... [έξι μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού] να θεσπίζει κατ' εξουσιοδότηση πράξεις σύμφωνα με το άρθρο 20α, για τη συμπλήρωση του παρόντος κανονισμού, καθορίζοντας τους όρους της εν λόγω διαλειτουργικότητας σε στενή συνεργασία με τα διασυνοριακά SOC και με βάση διεθνή πρότυπα και βέλτιστες πρακτικές της βιομηχανίας.

4. Τα διασυνοριακά SOC συνάπτουν συμφωνίες συνεργασίας μεταξύ τους ***και, κατά περίπτωση, με ISAC της βιομηχανίας***, προσδιορίζοντας τις αρχές ανταλλαγής πληροφοριών ***και διαλειτουργικότητας*** μεταξύ των διασυνοριακών πλατφορμών, ***λαμβάνοντας υπόψη τους υφιστάμενους σχετικούς μηχανισμούς ανταλλαγής πληροφοριών που προβλέπονται στην οδηγία (ΕΕ) 2022/2555***. ***Κατά περίπτωση, τα διασυνοριακά SOC συνάπτουν συμφωνίες συνεργασίας με ISAC της βιομηχανίας. Στο πλαίσιο πιθανού ή εν εξελίξει μεγάλης κλίμακας περιστατικού κυβερνοασφάλειας, οι μηχανισμοί ανταλλαγής πληροφοριών συμμορφώνονται με τις σχετικές διατάξεις της οδηγίας (ΕΕ) 2022/2555.***

Άρθρο 7

Συνεργασία και ανταλλαγή πληροφοριών με *το δίκτυο CSIRT*

1. Όταν τα διασυνοριακά SOC λαμβάνουν πληροφορίες σχετικά με δυνητικό ή εξελισσόμενο μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας ***για τον σκοπό της κοινής αντίληψης της κατάστασης, το SOC συντονισμού*** παρέχει σχετικές πληροφορίες ***στην CSIRT του ή στην αρμόδια αρχή, οι οποίες τις υποβάλλουν στο*** EU-CyCLONe, στο δίκτυο CSIRT και στην Επιτροπή ***και τον ENISA***, λαμβανομένων υπόψη των αντίστοιχων ρόλων τους όσον αφορά τη διαχείριση κρίσεων και τις διαδικασίες σύμφωνα με την οδηγία (ΕΕ) 2022/2555, χωρίς αδικαιολόγητη καθυστέρηση. ***Η παρούσα παράγραφος δεν επιβάλλει περαιτέρω υποχρεώσεις σε δημόσιες ή ιδιωτικές οντότητες όσον αφορά την κοινοποίηση δυνητικού ή εν εξελίξει περιστατικού μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας για την εκπλήρωση των υποχρεώσεων που ορίζονται στην οδηγία (ΕΕ) 2022/2555.***

2. ***Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις σύμφωνα με το άρθρο 20α κατόπιν διαβούλευσης με το δίκτυο CSIRT, για να συμπληρώνει τον παρόντα κανονισμό καθορίζοντας*** τις διαδικαστικές ρυθμίσεις για την ανταλλαγή πληροφοριών που προβλέπεται στην παράγραφο 1 ***του παρόντος άρθρου και σύμφωνα με την οδηγία (ΕΕ) 2022/2555***.

Άρθρο 8

Ασφάλεια

1. Τα κράτη μέλη που συμμετέχουν στην ευρωπαϊκή Κυβερνοασπίδα διασφαλίζουν υψηλό επίπεδο ***εμπιστευτικότητας και*** 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. ***Συμμορφώνονται με τις οδηγίες (ΕΕ) 2022/2555 και (ΕΕ) 2022/2557. Στις εν λόγω κατ' εξουσιοδότηση πράξεις,*** η Επιτροπή, υποστηριζόμενη από τον Ύπατο Εκπρόσωπο, λαμβάνει υπόψη τα σχετικά πρότυπα ασφάλειας σε επίπεδο άμυνας, προκειμένου να διευκολύνει τη συνεργασία με στρατιωτικούς φορείς.

Κεφάλαιο ΙΙΙ

ΜΗΧΑΝΙΣΜΟΣ ΕΚΤΑΚΤΗΣ ΑΝΑΓΚΗΣ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΣΦΑΛΕΙΑ

Άρθρο 9

Θέσπιση του Μηχανισμού έκτακτης ανάγκης *για την κυβερνοασφάλεια*

1. Θεσπίζεται Μηχανισμός έκτακτης ανάγκης ***για την κυβερνοασφάλεια*** 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 ▌ 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 ***διαχειριζόμενων υπηρεσιών ασφάλειας*** 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.

1α. Μετά την ενεργοποίηση του Μηχανισμού, η Επιτροπή αξιολογεί και δημοσιεύει, σε ετήσια βάση, έκθεση σχετικά με τα θετικά και τα αρνητικά σημεία της λειτουργίας του Μηχανισμού, συμπεριλαμβανομένης της ανάγκης για περαιτέρω συνεργασία ή για απαιτήσεις κατάρτισης.

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, σύμφωνα με τις ρυθμίσεις που έχουν θεσπιστεί για τα είδη οντοτήτων στους τομείς υψηλής κρισιμότητας που παρατίθενται στο παράρτημα Ι της οδηγίας (ΕΕ) 2022/2555.

2. Η ομάδα συνεργασίας NIS, σε συνεργασία με την Επιτροπή, τον ENISA, και τον Ύπατο Εκπρόσωπο ***και τις οντότητες που υπόκεινται σε συντονισμένες δοκιμές ετοιμότητας σύμφωνα με την παράγραφο 1***, αναπτύσσει κοινά σενάρια κινδύνου και μεθοδολογίες για τις συντονισμένες ασκήσεις δοκιμών ***ετοιμότητας***, ***βάσει των οποίων καταρτίζεται συντονισμένο σχέδιο εργασίας***. ***Οι οντότητες που υπόκεινται σε συντονισμένες δοκιμές ετοιμότητας καταρτίζουν και εφαρμόζουν σχέδιο αποκατάστασης το οποίο υλοποιεί τις συστάσεις από τις δοκιμές ετοιμότητας.***

Η ομάδα συνεργασίας NIS μπορεί να ενημερώνει σχετικά με την ιεράρχηση των τομέων ή υποτομέων για τις συντονισμένες ασκήσεις δοκιμών ετοιμότητας.

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 κυβερνοασφάλειας και την άμεση ανάκαμψη από τέτοια περιστατικά.

Όταν είναι προφανές ότι οι υπηρεσίες που αποτελούν αντικείμενο της σύμβασης δεν μπορούν να χρησιμοποιηθούν πλήρως για τους σκοπούς της παροχής στήριξης για την αντιμετώπιση σημαντικών ή μεγάλης κλίμακας συμβάντων, οι εν λόγω υπηρεσίες μπορούν κατ' εξαίρεση να μετατραπούν σε ασκήσεις ή προγράμματα κατάρτισης για την αντιμετώπιση συμβάντων, και να παρασχεθούν στους χρήστες κατόπιν αιτήματος, από την αναθέτουσα αρχή.

2. Η Εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας συνίσταται σε υπηρεσίες αντιμετώπισης περιστατικών από αξιόπιστους παρόχους ***υπηρεσιών διαχείρισης κινδύνων κυβερνοασφάλειας*** που επιλέγονται σύμφωνα με τα κριτήρια που ορίζονται στο άρθρο 16. Η ***Εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας*** περιλαμβάνει προκαθορισμένες υπηρεσίες. Οι υπηρεσίες μπορούν να αναπτύσσονται σε όλα τα κράτη μέλη, ***ενισχύουν την τεχνολογική κυριαρχία της Ένωσης, την ανοικτή στρατηγική αυτονομία, την ανταγωνιστικότητα και την ανθεκτικότητά της στον τομέα της κυβερνοασφάλειας, μεταξύ άλλων δίνοντας ώθηση στην καινοτομία στην ψηφιακή ενιαία αγορά σε ολόκληρη την Ένωση***.

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) θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης ***που αναφέρονται στο άρθρο 3 παράγραφος 1 του κανονισμού (ΕΕ).../2023 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[27] και το CERT-ΕΕ***.

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, ***σε συντονισμό με την ομάδα συντονισμού NIS2 και*** 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 ***αναθέτει*** 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 απαιτούμενων υπηρεσιών, ***συμπεριλαμβανομένων των αναγκαίων δεξιοτήτων και ικανοτήτων του εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας,*** κατόπιν διαβούλευσης με τα κράτη μέλη και την Επιτροπή ***και, κατά περίπτωση, με τους παρόχους υπηρεσιών διαχείρισης κινδύνων κυβερνοασφάλειας και άλλους εκπροσώπους του κλάδου της κυβερνοασφάλειας.*** Ο ENISA καταρτίζει παρόμοια χαρτογράφηση, κατόπιν διαβούλευσης με την Επιτροπή***, τους παρόχους υπηρεσιών διαχείρισης κυβερνοασφάλειας και, κατά περίπτωση, άλλους εκπροσώπους του κλάδου της κυβερνοασφάλειας,*** για τον προσδιορισμό των αναγκών 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, διαβουλεύεται με τον Ύπατο Εκπρόσωπο ***και ενημερώνει το Συμβούλιο σχετικά με τις ανάγκες τρίτων χωρών.***

8. Ανατίθεται στην Επιτροπή ***η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις σύμφωνα με το άρθρο 20α για να συμπληρώνει τον παρόντα κανονισμό καθορίζοντας*** τα είδη και τον αριθμό των υπηρεσιών αντιμετώπισης που απαιτούνται για την Εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας. ▌..

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 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

---

27 ***Κανονισμός (ΕΕ) .../2023 για τον καθορισμό μέτρων για υψηλό κοινό επίπεδο κυβερνοασφάλειας στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης (ΕΕ C της , σ. , ELI: ...).***

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. ***Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις σύμφωνα με το άρθρο 20α για να συμπληρώνει τον παρόντα κανονισμό καθορίζοντας*** περαιτέρω τις λεπτομερείς ρυθμίσεις για την κατανομή των υπηρεσιών στήριξης της Εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. ▌

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 ***αμελλητί και εντός 24 ωρών***.

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) η κλίμακα και 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 της 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 ***και κάθε άλλη διάταξη την οποία τα μέρη της συμφωνίας θεωρούν αναγκαία για την παροχή της αντίστοιχης υπηρεσίας***.

4. Οι συμφωνίες που αναφέρονται στην παράγραφο 3 βασίζονται σε υποδείγματα που καταρτίζει ο ENISA, αφού ζητήσει τη γνώμη των κρατών μελών ***και***, ***όπου είναι σκόπιμο, άλλων χρηστών της Εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας***.

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***, με εξαίρεση περιπτώσεις βαριάς αμέλειας κατά την αξιολόγηση της εφαρμογής του παρόχου υπηρεσιών ή σε περίπτωση που η Επιτροπή ή ο ENISA είναι χρήστες της Εφεδρείας της ΕΕ για την κυβερνοασφάλεια σύμφωνα με το άρθρο 14 παράγραφος 3.***

6. Εντός ενός μηνός από το τέλος της δράσης στήριξης, οι χρήστες υποβάλλουν στην Επιτροπή, στον ENISA***, στο δίκτυο CSIRT και, κατά περίπτωση, στο EU-CyCLONe*** 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 Ύπατο Εκπρόσωπο.

Η έκθεση σέβεται το ενωσιακό και το εθνικό δίκαιο σχετικά με την προστασία ευαίσθητων ή διαβαθμισμένων πληροφοριών.

7. Η Επιτροπή υποβάλλει έκθεση ***σε τακτική βάση, τουλάχιστον δύο φορές τον χρόνο,*** στην ομάδα συνεργασίας NIS σχετικά με τη χρήση και τα αποτελέσματα της στήριξης. ***Προστατεύει τις εμπιστευτικές πληροφορίες, σύμφωνα με το ενωσιακό και το εθνικό δίκαιο σχετικά με την προστασία ευαίσθητων ή διαβαθμισμένων πληροφοριών.***

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[28], 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

[28] 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 Ύπατο Εκπρόσωπο, η στήριξη στο πλαίσιο του Μηχανισμού έκτακτης ανάγκης ***για την κυβερνοασφάλεια*** 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 ***ΣΕΕ***.

4. Η στήριξη στο πλαίσιο του Μηχανισμού έκτακτης ανάγκης ***για την κυβερνοασφάλεια*** 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, συμπεριλαμβανομένων της προώθησης της ανάπτυξης δεξιοτήτων κυβερνοασφάλειας στην ΕΕ ***και της επίτευξης ισόρροπης εκπροσώπησης των φύλων στον τομέα, και ενισχύοντας την τεχνολογική κυριαρχία, την ανοικτή στρατηγική αυτονομία, την ανταγωνιστικότητα και την ανθεκτικότητα της Ένωσης***.

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 επικαιροποιημένο τεχνικό εξοπλισμό υλισμικού και λογισμικού που απαιτείται για την υποστήριξη της αιτούμενης υπηρεσίας ***και συμμορφώνεται, κατά περίπτωση, με τον κανονισμο (ΕΕ) .../... του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[29] (2022/0272(COD)),***

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, ***ή σε μία από τις γλώσσες εργασίας των θεσμικών οργάνων της Ένωσης,*** όπου μπορεί να παρέχει την υπηρεσία,

ι) μόλις τεθεί σε εφαρμογή ένα ***ευρωπαϊκό σύστημα πιστοποίησης κυβερνοασφάλειας*** τις υπηρεσίες διαχείρισης κυβερνοασφάλειας ***σύμφωνα με*** τον κανονισμό (ΕΕ) 2019/881, ο πάροχος πιστοποιείται σύμφωνα με το εν λόγω σύστημα, ***εντός διαστήματος δύο ετών από την έγκριση του συστήματος***.

ι α) ο πάροχος πρέπει να είναι σε θέση να παρέχει την υπηρεσία ανεξάρτητα και όχι στο πλαίσιο δέσμης, διασφαλίζοντας έτσι τη δυνατότητα του χρήστη να αλλάζει πάροχο υπηρεσιών·

ι β) για τους σκοπούς του άρθρου 12 παράγραφος 1, ο πάροχος περιλαμβάνει στην πρόταση υποβολής προσφορών τη δυνατότητα μετατροπής των αχρησιμοποίητων υπηρεσιών αντιμετώπισης περιστατικών σε ασκήσεις ή προγράμματα κατάρτισης·

ι γ) ο πάροχος είναι εγκατεστημένος και διαθέτει τις δομές εκτελεστικής διαχείρισής του στην Ένωση, σε συνδεδεμένη χώρα ή σε τρίτη χώρα που αποτελεί μέρος της συμφωνίας για τις δημόσιες συμβάσεις στο πλαίσιο του Παγκόσμιου Οργανισμού Εμπορίου (ΣΔΣ).

ι δ) Ο πάροχος δεν υπόκειται σε έλεγχο από μη συνδεδεμένη τρίτη χώρα ή από οντότητα μη συνδεδεμένης τρίτης χώρας που δεν είναι συμβαλλόμενο μέρος της ΣΔΣ ή, εναλλακτικά, η εν λόγω οντότητα έχει υποβληθεί σε έλεγχο κατά την έννοια του κανονισμού (ΕΕ) 2019/452 και, κατά περίπτωση, σε μέτρα μετριασμού, λαμβανομένων υπόψη των στόχων που ορίζονται στον παρόντα κανονισμό.

Άρθρο 17

Στήριξη σε τρίτες χώρες

---

29 Κανονισμός (ΕΕ) .../... του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της ... σχετικά με ... (ΕΕ L της, ELI: …).

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 Ύπατο 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 ***ενημερώνει αμελλητί το Συμβούλιο και*** συντονίζει με τον Ύπατο 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 εξετάζει και να αξιολογεί απειλές, ευπάθειες 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 Ύπατο Εκπρόσωπο.

2. Για την εκπόνηση της έκθεσης εξέτασης περιστατικού που αναφέρεται στην παράγραφο 1, ο ENISA συνεργάζεται με όλα τα σχετικά ενδιαφερόμενα μέρη ***και συλλέγει στοιχεία από αυτά***, συμπεριλαμβανομένων εκπροσώπων των κρατών μελών, της Επιτροπής, άλλων σχετικών θεσμικών και λοιπών οργάνων ***και οργανισμών*** της ΕΕ, παρόχων υπηρεσιών διαχείρισης κυβερνοασφάλειας στα ***εθνικά και διασυνοριακά***SOC και χρηστών υπηρεσιών κυβερνοασφάλειας***, σε συνδυασμό με επαρκείς εγγυήσεις και παρακολούθηση ώστε να διασφαλίζεται ότι τα διδάγματα που αντλούνται και οι βέλτιστες πρακτικές που***

προσδιορίζονται υποστηρίζονται από τους παράγοντες του κλάδου των 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 ευπαθειών 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. ***Δεν περιλαμβάνει λεπτομέρειες σχετικά με ευπάθειες που αποτελούν αντικείμενο ενεργού εκμετάλλευσης και δεν έχουν ακόμα αρθεί.***

3α. Η έκθεση που αναφέρεται στην παράγραφο 1 του παρόντος άρθρου εκθέτει τα διδάγματα που αντλήθηκαν από τις αξιολογήσεις από ομοτίμους που διενεργήθηκαν σύμφωνα με το άρθρο 19 της οδηγίας (ΕΕ) 2022/2555.

4. Κατά περίπτωση, η έκθεση διατυπώνει συστάσεις***, μεταξύ άλλων για όλα τα σχετικά ενδιαφερόμενα μέρη***, για τη βελτίωση της κατάστασης κυβερνοασφάλειας της Ένωσης·

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:

i) προστίθεται το ακόλουθο στοιχείο αα):

«αα) στήριξη της ανάπτυξης ενωσιακής Κυβερνοασπίδας, συμπεριλαμβανομένων 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 κυβερνοαπειλές»·

ii) προστίθεται το ακόλουθο στοιχείο ζ):

«ζ) σύσταση και λειτουργία Μηχανισμού έκτακτης ανάγκης για ***την κυβερνοασφάλεια*** 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.»·

β) 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*, με εξαίρεση τις δράσεις για την υλοποίηση της Εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, η οποία υλοποιείται από την Επιτροπή και τον ENISA.

_____

* 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, ***ELI: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32021R0887).'·***

(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) ***1 620 566 000*** EUR για τον ειδικό στόχο 3 – Κυβερνοασφάλεια και εμπιστοσύνη,

δ) ***500 347 000*** EUR για τον ειδικό στόχο 4 – Προηγμένες ψηφιακές δεξιότητες»·

αα) παρεμβάλλεται η ακόλουθη νέα παράγραφος 2α:

«(2α). Το ποσό που αναφέρεται στην παράγραφο 2 στοιχείο γ) χρησιμοποιείται πρωτίστως για την επίτευξη των επιχειρησιακών στόχων που αναφέρονται στο άρθρο 6 παράγραφος 1 στοιχεία α-στ) του προγράμματος.»·

αβ) παρεμβάλλεται η ακόλουθη νέα παράγραφος 2β:

«(2β). Το ποσό για τη σύσταση και την υλοποίηση της Εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας δεν υπερβαίνει τα 27 εκατομμύρια για την προβλεπόμενη διάρκεια ισχύος του κανονισμού σχετικά με τον καθορισμό μέτρων για την ενίσχυση της αλληλεγγύης και των ικανοτήτων της Ένωσης να εντοπίζει, να προετοιμάζεται για και να αντιμετωπίζει απειλές και περιστατικά κυβερνοασφάλειας»·

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 ***στο πλαίσιο της εφαρμογής της Εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας***, 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.·

Η Επιτροπή ενημερώνει το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο σχετικά με τις μεταφερόμενες πιστώσεις αναλήψεων υποχρεώσεων σύμφωνα με το άρθρο 12 παράγραφος 6 του κανονισμού (ΕΕ, Ευρατόμ) 2018/1046.

(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 κανονισμό ***(ΕΕ, Ευρατόμ) 2018/1046***, 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/ΕΕ[27] και 2014/25/ΕΕ[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/**...**, 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 ενοικίων, στις εν λόγω τρίτες χώρες. Κατά παρέκκλιση από το άρθρο 169 παράγραφος 3 του κανονισμού (ΕΕ) **…/…**, 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/**...**, 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) **…/…**, 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:

«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/**….** Σε περίπτωση σύγκρουσης των διατάξεων του παρόντος κανονισμού με τις διατάξεις των άρθρων 4 και 5 του κανονισμού (ΕΕ) 2023/**….**, 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 κανονισμού ***(ΕΕ, Ευρατόμ) 2018/1046*** 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 κανονισμού ***(ΕΕ, Ευρατόμ) 2016/1046***. 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 ***(ΕΕ) .../....*** και την κοινοπραξία υποδοχής που αναφέρεται στο άρθρο 5 του κανονισμού ***(ΕΕ) .../...***, σύμφωνα με το άρθρο 195 παράγραφος 1 στοιχείο δ) του κανονισμού ***(ΕΕ, Ευρατόμ) 2018/1046***.

Στήριξη με τη μορφή επιχορηγήσεων για τον Μηχανισμό έκτακτης ανάγκης ***για την κυβερνοασφάλεια***, όπως ορίζεται στο άρθρο 10 του κανονισμού ***(ΕΕ)***, μπορεί να χορηγείται απευθείας από το ECCC στα κράτη μέλη χωρίς πρόσκληση υποβολής προτάσεων, σύμφωνα με το άρθρο 195 παράγραφος 1 στοιχείο δ) του ***κανονισμού (ΕΕ, Ευρατόμ) 2018/1046***.

Για τις δράσεις που προσδιορίζονται στο άρθρο 10 παράγραφος 1 στοιχείο γ) του κανονισμού ***(ΕΕ) .../...***,, 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 ***(ΕΕ) .../...***, και σύμφωνα με το άρθρο 193 παράγραφος 2 δεύτερο εδάφιο στοιχείο α) του κανονισμού ***(ΕΕ, Ευρατόμ) 2018/1046***, 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 του κανονισμού (ΕΕ) 2021/694 τροποποιούνται σύμφωνα με το παράρτημα του παρόντος κανονισμού.

Άρθρο 19α

Πρόσθετοι πόροι για τον ENISA

Ο ENISA λαμβάνει πρόσθετους πόρους για την εκτέλεση των πρόσθετων καθηκόντων του που του ανατίθενται με τον παρόντα κανονισμό. Η εν λόγω πρόσθετη στήριξη, συμπεριλαμβανομένης της χρηματοδότησης, δεν θέτει σε κίνδυνο την επίτευξη των στόχων άλλων προγραμμάτων της Ένωσης, ιδίως του προγράμματος «Ψηφιακή Ευρώπη».

Άρθρο 20

Αξιολόγηση *και επανεξέταση*

1. Έως [***δύο*** έτη ***από*** την ημερομηνία εφαρμογής του παρόντος κανονισμού ***και ακολούθως ανά δύο έτη***], η Επιτροπή ***πραγματοποιεί αξιολόγηση της λειτουργίας των μέτρων που ορίζονται στον παρόντα κανονισμό και*** υποβάλλει ***έκθεση*** στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο.

2. Πιο συγκεκριμένα, στο πλαίσιο της αξιολόγησης αποτιμώνται:

α) η χρήση και η προστιθέμενη αξία των διασυνοριακών SOC και τον βαθμό στον οποίο συμβάλλουν στην επιτάχυνση του εντοπισμού και της αντιμετώπισης

κυβερνοαπειλών και στην επίγνωση της κατάστασης· η ενεργός συμμετοχή των εθνικών SOC στην ευρωπαϊκή Κυβερνοασπίδα, συμπεριλαμβανομένων του αριθμού των εθνικών SOC και των διασυνοριακών SOC που έχουν συσταθεί και του βαθμού στον οποίο έχει συμβάλει στην παραγωγή και ανταλλαγή αξιοποιήσιμων πληροφοριών υψηλής ποιότητας και πληροφοριών για κυβερνοαπειλές· ο αριθμός υποδομών ή εργαλείων κυβερνοασφάλειας, ή και των δύο, που αποκτώνται με κοινές συμβάσεις· ο αριθμός συμφωνιών συνεργασίας που έχουν συναφθεί μεταξύ διασυνοριακών SOC και κλαδικών ISAC· ο αριθμός των συμβάντων που αναφέρθηκαν στο δίκτυο CSIRT και ο αντίκτυπός του στο έργο του δικτύου CSIRT·

β) τόσο η θετική όσο και η αρνητική λειτουργία του μηχανισμού έκτακτης ανάγκης στον τομέα της κυβερνοασφάλειας, συμπεριλαμβανομένου του κατά πόσον απαιτούνται περαιτέρω απαιτήσεις συνεργασίας ή κατάρτισης·

γ) η συμβολή του παρόντος κανονισμού στην ενίσχυση της ανθεκτικότητας και της ανοικτής στρατηγικής αυτονομίας της Ένωσης, στη βελτίωση της ανταγωνιστικότητας των σχετικών βιομηχανικών τομέων, των πολύ μικρών επιχειρήσεων και των ΜΜΕ, συμπεριλαμβανομένων των νεοφυών επιχειρήσεων, και στην ανάπτυξη δεξιοτήτων κυβερνοασφάλειας στην Ένωση·

δ) η χρήση και η προστιθέμενη αξία της Εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, συμπεριλαμβανομένου του αριθμού των αξιόπιστων παρόχων ασφάλειας που αποτελούν μέρος της Εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας· ο αριθμός, το είδος, το κόστος και ο αντίκτυπος των δράσεων που υλοποιούνται για την υποστήριξη της αντιμετώπισης περιστατικών κυβερνοασφάλειας, καθώς και των χρηστών και των παρόχων τους· ο μέσος χρόνος που χρειάζονται η Επιτροπή για να αναγνωρίσει, η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας για να αναπτυχθεί και να αντιδράσει, και ο χρήστης για να ανακάμψει από περιστατικά· το κατά πόσον το πεδίο εφαρμογής της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας πρέπει να διευρυνθεί ώστε να περιλαμβάνει υπηρεσίες ετοιμότητας για συμβάντα ή κοινές ασκήσεις με τους αξιόπιστους παρόχους υπηρεσιών διαχείρισης κυβερνοασφάλειας και τους δυνητικούς χρήστες της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, ώστε να διασφαλίζεται η αποδοτική λειτουργία της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, όπου απαιτείται·

ε) η συμβολή του παρόντος κανονισμού στην ανάπτυξη και βελτίωση των δεξιοτήτων και ικανοτήτων του εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας, η οποία είναι αναγκαία για την ενίσχυση της ικανότητας της Ένωσης στην ανίχνευση, πρόληψη και αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας και στην ανάκαμψη από αυτά·

στ) η συμβολή του παρόντος κανονισμού στην εφαρμογή και ανάπτυξη τεχνολογιών αιχμής στην Ένωση.

3. Βάσει των εκθέσεων που αναφέρονται στην παράγραφο 1, η Επιτροπή υποβάλλει, κατά περίπτωση, νομοθετική πρόταση στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο για την τροποποίηση του παρόντος κανονισμού.

Άρθρο 20α

Άσκηση της εξουσιοδότησης

1. Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις υπό τους όρους του παρόντος άρθρου.

2. Η προβλεπόμενη στο άρθρο 6 παράγραφος 3, στο άρθρο 7 παράγραφος 2, στο άρθρο 12 παράγραφος 8 και στο άρθρο 13 παράγραφος 7 εξουσία έκδοσης κατ' εξουσιοδότηση πράξεων ανατίθεται στην Επιτροπή για χρονικό διάστημα ... ετών από την/τις ... [ημερομηνία έναρξης ισχύος της βασικής νομοθετικής πράξης ή οποιαδήποτε άλλη ημερομηνία ορίζουν οι συννομοθέτες]. Η Επιτροπή υποβάλλει έκθεση σχετικά με τις εξουσίες που της έχουν ανατεθεί το αργότερο εννέα μήνες πριν από τη λήξη της περιόδου των … ετών. Η εξουσιοδότηση ανανεώνεται σιωπηρά για περιόδους ίδιας διάρκειας, εκτός αν το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο προβάλλει αντιρρήσεις το αργότερο τρεις μήνες πριν από τη λήξη της κάθε περιόδου.

3. Η εξουσιοδότηση που προβλέπεται στο άρθρο 6 παράγραφος 3, στο άρθρο 7 παράγραφος 2, στο άρθρο 12 παράγραφος 8 και στο άρθρο 13 παράγραφος 7 μπορεί να ανακληθεί ανά πάσα στιγμή από το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο. Η απόφαση ανάκλησης περατώνει την εξουσιοδότηση που προσδιορίζεται στην εν λόγω απόφαση. Αρχίζει να ισχύει την επομένη της δημοσίευσης της απόφασης στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης ή σε μεταγενέστερη ημερομηνία που ορίζεται σε αυτή. Δεν θίγει το κύρος των κατ' εξουσιοδότηση πράξεων που ισχύουν ήδη.

4. Πριν από την έκδοση μιας κατ' εξουσιοδότηση πράξης, η Επιτροπή διεξάγει διαβουλεύσεις με εμπειρογνώμονες που ορίζουν τα κράτη μέλη σύμφωνα με τις αρχές της διοργανικής συμφωνίας της 13ης Απριλίου 2016 για τη βελτίωση του νομοθετικού έργου.

5. Μόλις εκδώσει μια κατ' εξουσιοδότηση πράξη, η Επιτροπή την κοινοποιεί ταυτόχρονα στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο.

6. Κάθε κατ' εξουσιοδότηση πράξη που εκδίδεται σύμφωνα με το άρθρο 6 παράγραφος 3, το άρθρο 7 παράγραφος 2, το άρθρο 12 παράγραφος 8 ή το άρθρο 13 παράγραφος 7 αρχίζει να ισχύει μόνον εφόσον δεν διατυπωθούν αντιρρήσεις είτε από το Ευρωπαϊκό Κοινοβούλιο είτε από το Συμβούλιο εντός προθεσμίας δύο μηνών από την κοινοποίηση της πράξης στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο ή εάν, πριν λήξει αυτή η προθεσμία, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο ενημερώσουν αμφότερα την Επιτροπή ότι δεν πρόκειται να προβάλουν αντίρρηση. Η προθεσμία αυτή παρατείνεται κατά [δύο μήνες] κατόπιν πρωτοβουλίας του Ευρωπαϊκού Κοινοβουλίου ή του Συμβουλίου.

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.

…,

Για το Ευρωπαϊκό Κοινοβούλιο	*Για το Συμβούλιο*
Η Πρόεδρος	*Ο/Η Πρόεδρος*

ΠΑΡΑΡΤΗΜΑ

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

(1) στο παράρτημα ΙΙ, το τμήμα/κεφάλαιο «Ειδικός στόχος 3 – Κυβερνοασφάλεια και εμπιστοσύνη» αντικαθίσταται από το ακόλουθο κείμενο:

«Ειδικός στόχος 3 – Κυβερνοασφάλεια και εμπιστοσύνη

Το πρόγραμμα προάγει την ενίσχυση, την οικοδόμηση και την απόκτηση ουσιωδών δυνατοτήτων για τη θωράκιση της ψηφιακής οικονομίας, της κοινωνίας και της δημοκρατίας της Ένωσης, ενισχύοντας το βιομηχανικό δυναμικό και την ανταγωνιστικότητα της Ένωσης στον τομέα της κυβερνοασφάλειας, καθώς και βελτιώνοντας τις ικανότητες τόσο του ιδιωτικού όσο και του δημόσιου τομέα για την προστασία των πολιτών και των επιχειρήσεων από κυβερνοαπειλές, μεταξύ άλλων με στήριξη της εφαρμογής της οδηγίας (ΕΕ) 2016/1148.

Στις αρχικές και, κατά περίπτωση, στις επακόλουθες δράσεις του παρόντος στόχου περιλαμβάνονται:

1. Συνεπένδυση με τα κράτη μέλη σε προηγμένο εξοπλισμό, υποδομές και τεχνογνωσία κυβερνοασφάλειας που είναι ουσιώδεις για την προστασία των υποδομών ζωτικής σημασίας και της ψηφιακής ενιαίας αγοράς γενικότερα. Η εν λόγω συνεπένδυση θα μπορούσε να περιλαμβάνει επενδύσεις σε κβαντικές εγκαταστάσεις και πόρους δεδομένων για την κυβερνοασφάλεια, την επίγνωση της κατάστασης στον κυβερνοχώρο ***συμπεριλαμβανομένων των εθνικών SOC και των διασυνοριακών SOC που απαρτίζουν την ευρωπαϊκή Κυβερνοασπίδα***, καθώς και άλλα εργαλεία που θα τίθενται στη διάθεση του δημόσιου και του ιδιωτικού τομέα σε ολόκληρη την Ευρώπη.

2. Κλιμάκωση των υφιστάμενων τεχνολογικών δυνατοτήτων, δικτύωση των κέντρων ικανοτήτων στα κράτη μέλη και μέριμνα ώστε οι εν λόγω δυνατότητες να ανταποκρίνονται στις ανάγκες του δημόσιου τομέα και του βιομηχανικού κλάδου, μεταξύ άλλων για προϊόντα και υπηρεσίες που ενισχύουν την κυβερνοασφάλεια και την εμπιστοσύνη εντός της ψηφιακής ενιαίας αγοράς.

3. Εξασφάλιση της ευρείας ανάπτυξης αποτελεσματικών λύσεων αιχμής στους τομείς της κυβερνοασφάλειας και της εμπιστοσύνης σε όλα τα κράτη μέλη. Η εν λόγω ανάπτυξη περιλαμβάνει την ενίσχυση της προστασίας και της ασφάλειας των προϊόντων, από τον σχεδιασμό τους έως τη διάθεσή τους στο εμπόριο.

4. Παροχή στήριξης για να εξαλειφθεί το χάσμα δεξιοτήτων κυβερνοασφάλειας, ***με ιδιαίτερη έμφαση στην επίτευξη ισόρροπης εκπροσώπησης των φύλων***, για παράδειγμα με την ευθυγράμμιση των προγραμμάτων για τις δεξιότητες κυβερνοασφάλειας, την προσαρμογή τους σε συγκεκριμένες τομεακές ανάγκες, ***συμπεριλαμβανομένης διεπιστημονικής και γενικής εστίασης*** και τη διευκόλυνση της πρόσβασης σε στοχευμένη εξειδικευμένη κατάρτιση ***που θα ενδυναμώνει όλα τα πρόσωπα και τα εδάφη, με την επιφύλαξη της δυνατότητας αξιοποίησης των ευκαιριών που παρέχει ο παρών κανονισμός***.

5. Προώθηση της αλληλεγγύης μεταξύ των κρατών μελών όσον αφορά την προετοιμασία και την αντιμετώπιση σημαντικών περιστατικών στον τομέα της κυβερνοασφάλειας μέσω της ανάπτυξης υπηρεσιών κυβερνοασφάλειας σε διασυνοριακό επίπεδο, συμπεριλαμβανομένης της στήριξης για αμοιβαία συνδρομή μεταξύ των δημόσιων αρχών και της δημιουργίας Εφεδρείας αξιόπιστων παρόχων ***υπηρεσιών διαχείρισης κυβερνοασφάλειας*** σε επίπεδο Ένωσης.»·

(2) στο παράρτημα ΙΙ, το τμήμα/κεφάλαιο «Ειδικός στόχος 3 – Κυβερνοασφάλεια και εμπιστοσύνη» αντικαθίσταται από το ακόλουθο κείμενο:

«Ειδικός στόχος 3 – Κυβερνοασφάλεια και εμπιστοσύνη

3.1. Ο αριθμός υποδομών ή εργαλείων κυβερνοασφάλειας, ή και των δύο, που αποκτώνται με κοινές συμβάσεις ***στο πλαίσιο της Κυβερνοασπίδας.***

3.2. Ο αριθμός χρηστών και κοινοτήτων χρηστών που αποκτούν πρόσβαση σε ευρωπαϊκά μέσα κυβερνοασφάλειας

3.3. Ο αριθμός***, ο τύπος, το κόστος και ο αντίκτυπος*** των δράσεων που ***αναλαμβάνονται*** για τη στήριξη της ετοιμότητας και της αντιμετώπισης περιστατικών κυβερνοασφάλειας στο πλαίσιο του Μηχανισμού έκτακτης ανάγκης ***για την κυβερνοασφάλεια***. ***Ο βαθμός στον οποίο οι συστάσεις δοκιμών ετοιμότητας εφαρμόστηκαν και υιοθετήθηκαν από τον χρήστη, καθώς και ο μέσος χρόνος που χρειάστηκαν η Επιτροπή για να εντοπίσει, η Εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας για να αντιδράσει, και ο χρήστης για να ανακάμψει από συμβάντα.»***