Συμβούλιο της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 18 Νοεμβρίου 2024
(OR. en)

15644/24

**Διοργανικός φάκελος:**
**2023/0109(COD)**

**CODEC 2118**
**CYBER 326**
**TELECOM 335**
**CADREFIN 188**
**FIN 1009**
**BUDGET 63**
**IND 514**
**JAI 1656**
**MI 926**
**DATAPROTECT 318**
**RELEX 1429**
**PE 252**

**ΕΝΗΜΕΡΩΤΙΚΟ ΣΗΜΕΙΩΜΑ**

| | |
|---|---|
| Αποστολέας: | Γενική Γραμματεία του Συμβουλίου |
| Αποδέκτης: | Επιτροπή των Μονίμων Αντιπροσώπων / Συμβούλιο |
| Θέμα: | Πρόταση ΚΑΝΟΝΙΣΜΟΥ 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<br>- Αποτελέσματα της πρώτης ανάγνωσης στο Ευρωπαϊκό Κοινοβούλιο και διαδικασία έκδοσης διορθωτικού<br>(Στρασβούργο, 24 Απριλίου 2024 και Βρυξέλλες, 14 Νοεμβρίου 2024) |

## I. ΕΙΣΑΓΩΓΗ

Σύμφωνα με τις διατάξεις του άρθρου 294 της ΣΛΕΕ και την κοινή δήλωση σχετικά με την εφαρμογή στην πράξη της διαδικασίας συναπόφασης[1], πραγματοποιήθηκε σειρά άτυπων επαφών μεταξύ του Συμβουλίου, του Ευρωπαϊκού Κοινοβουλίου και της Επιτροπής, με σκοπό να επιτευχθεί συμφωνία επί του νομοθετικού φακέλου σε πρώτη ανάγνωση.

[1] ΕΕ C 145 της 30.6.2007, σ. 5.

Ο φάκελος αυτός αναμενόταν να υποβληθεί[2] στη διαδικασία έκδοσης διορθωτικού[3] στο Ευρωπαϊκό Κοινοβούλιο μετά την έγκριση από το απερχόμενο Ευρωπαϊκό Κοινοβούλιο της θέσης του σε πρώτη ανάγνωση.

## II. ΨΗΦΟΙ

Κατά τη συνεδρίασή του στις 24 Απριλίου 2024, το Ευρωπαϊκό Κοινοβούλιο ενέκρινε την τροπολογία 2 (χωρίς αναθεώρηση από τους γλωσσομαθείς νομικούς) στην πρόταση της Επιτροπής, την τροπολογία 3 που περιέχει δήλωση της Επιτροπής και ένα νομοθετικό ψήφισμα, τα οποία συνιστούν τη θέση του Ευρωπαϊκού Κοινοβουλίου σε πρώτη ανάγνωση. Η θέση αυτή απηχεί όσα είχαν συμφωνηθεί προσωρινά μεταξύ των θεσμικών οργάνων.

Μετά την οριστική διατύπωση του εγκριθέντος κειμένου από τους γλωσσομαθείς νομικούς, στις 14 Νοεμβρίου 2024 το Ευρωπαϊκό Κοινοβούλιο ενέκρινε διορθωτικό επί της θέσης που είχε καθοριστεί σε πρώτη ανάγνωση.

Με το διορθωτικό αυτό, το Συμβούλιο αναμένεται να είναι σε θέση να εγκρίνει τη θέση του Ευρωπαϊκού Κοινοβουλίου, ως έχει στο παράρτημα[4], ολοκληρώνοντας έτσι την πρώτη ανάγνωση και για τα δύο θεσμικά όργανα.

Ακολούθως η πράξη θα εκδοθεί με τη διατύπωση που αντιστοιχεί στη θέση του Ευρωπαϊκού Κοινοβουλίου.

---

[2] 10819/24 + COR 1

[3] Άρθρο 251 του κανονισμού του ΕΚ.

[4] Το κείμενο του διορθωτικού παρατίθεται στο παράρτημα, Παρατίθεται με τη μορφή ενοποιημένου κειμένου, όπου οι αλλαγές στην πρόταση της Επιτροπής επισημαίνονται με έντονα και πλάγια στοιχεία. Οι διαγραφές επισημαίνονται με το σύμβολο « ▌ ».

# P9_TA(2024)0355

## Κανονισμός για την αλληλεγγύη στον κυβερνοχώρο

**Νομοθετικό ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 24ης Απριλίου 2024 σχετικά με την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου που αφορά 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 [COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)]**

**(Συνήθης νομοθετική διαδικασία: πρώτη ανάγνωση)**

*Το Ευρωπαϊκό Κοινοβούλιο,*

– έχοντας υπόψη την πρόταση της Επιτροπής προς το Κοινοβούλιο και το Συμβούλιο [COM(2023)0209],

– έχοντας υπόψη το άρθρο 294 παράγραφος 2, το άρθρο 173 παράγραφος 3 και το άρθρο 322 παράγραφος 1 στοιχείο α) της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης, σύμφωνα με τα οποία του υποβλήθηκε η πρόταση από την Επιτροπή (C9-0136/2023),

– έχοντας υπόψη το άρθρο 294 παράγραφος 3 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης,

– έχοντας υπόψη τη γνώμη του Ελεγκτικού Συνεδρίου της 18ης Απριλίου 2023[1],

– έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής της 13ης Ιουλίου 2023[2],

– έχοντας υπόψη τη γνώμη της Επιτροπής των Περιφερειών της 30ής Νοεμβρίου 2023[3],

– έχοντας υπόψη την προσωρινή συμφωνία που εγκρίθηκε από την αρμόδια επιτροπή σύμφωνα με το άρθρο 74 παράγραφος 4 του Κανονισμού του και τη δέσμευση του εκπροσώπου του Συμβουλίου, με επιστολή της 21ης Μαρτίου 2024, να εγκρίνει τη θέση του Κοινοβουλίου, σύμφωνα με το άρθρο 294 παράγραφος 4 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης,

– έχοντας υπόψη το άρθρο 59 του Κανονισμού του,

– έχοντας υπόψη τις γνωμοδοτήσεις της Επιτροπής Εξωτερικών Υποθέσεων και της Επιτροπής Μεταφορών και Τουρισμού,

– έχοντας υπόψη την έκθεση της Επιτροπής Βιομηχανίας, Έρευνας και Ενέργειας (A9-0426/2023),

---

1 Δεν έχει ακόμη δημοσιευτεί στην Επίσημη Εφημερίδα.
2 ΕΕ C 349 της 29.9.2023, σ. 167.
3 ΕΕ C, C/2024/1049, 9.2.2024, ELI: http://data.europa.eu/eli/C/2024/1049/oj.

1. εγκρίνει τη θέση του σε πρώτη ανάγνωση όπως παρατίθεται κατωτέρω·

2. λαμβάνει υπό σημείωση τη δήλωση της Επιτροπής που επισυνάπτεται στο παρόν ψήφισμα, η οποία θα δημοσιευθεί στη σειρά C της *Επίσημης Εφημερίδας της Ευρωπαϊκής Ένωσης*·

3. ζητεί από την Επιτροπή να υποβάλει εκ νέου την πρόταση στο Κοινοβούλιο, αν την αντικαταστήσει με νέο κείμενο, αν της επιφέρει σημαντικές τροποποιήσεις ή αν προτίθεται να της επιφέρει σημαντικές τροποποιήσεις·

4. αναθέτει στην Πρόεδρό του να διαβιβάσει τη θέση του Κοινοβουλίου στο Συμβούλιο, στην Επιτροπή και στα εθνικά κοινοβούλια.

**P9_TC1-COD(2023)0109**

**Θέση του Ευρωπαϊκού Κοινοβουλίου που καθορίστηκε σε πρώτη ανάγνωση στις 24 Απριλίου 2024 εν όψει της έγκρισης κανονισμού (ΕΕ) 2024/... του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τον καθορισμό μέτρων για την ενίσχυση της αλληλεγγύης και των ικανοτήτων της Ένωσης για την ανίχνευση, την προετοιμασία και την αντιμετώπιση κυβερνοαπειλών και περιστατικών κυβερνοασφάλειας *και για την τροποποίηση του κανονισμού (ΕΕ) 2021/694 (κανονισμός για την αλληλεγγύη στον κυβερνοχώρο)***

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[4],

---

1 ***Γνώμη της 18ης Απριλίου 2023 (δεν έχει ακόμη δημοσιευτεί στην Επίσημη Εφημερίδα).***

2 ΕΕ C 349 της 29.9.2023, σ. 167.

3 ΕΕ C, C/2024/1049, 9.2.2024, ELI: http://data.europa.eu/eli/C/2024/1049/oj.

4 Θέση του Ευρωπαϊκού Κοινοβουλίου της 24ης Απριλίου 2024.

Εκτιμώντας τα ακόλουθα:

(1) Η χρήση των τεχνολογιών πληροφοριών και επικοινωνιών και η εξάρτηση από αυτές είναι πλέον θεμελιώδεις πτυχές σε όλους τους τομείς της οικονομικής δραστηριότητας ***και της κοινωνίας***, υπό το πρίσμα της συνεχώς αυξανόμενης διασυνδεσιμότητας και αλληλεξάρτησης των δημόσιων διοικήσεων, των επιχειρήσεων και των πολιτών των κρατών μελών, πέρα από τομείς και σύνορα***, γεγονός που συνεπάγεται ταυτόχρονα πιθανές ευπάθειες***.

(2) Το μέγεθος, η συχνότητα και οι επιπτώσεις των περιστατικών κυβερνοασφάλειας, συμπεριλαμβανομένων των επιθέσεων στην αλυσίδα εφοδιασμού με σκοπό την κυβερνοκατασκοπεία, την εγκατάσταση λυτρισμικού ή την πρόκληση διαταραχών, αυξάνονται ***τόσο σε επίπεδο Ένωσης όσο και παγκόσμια***. Αποτελούν μείζονα απειλή για τη λειτουργία των συστημάτων δικτύου και πληροφοριών. Ενόψει του ταχέως εξελισσόμενου τοπίου των απειλών, η απειλή πιθανών περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας που προκαλούν σημαντική διαταραχή ή ζημία σε κρίσιμες υποδομές απαιτεί αυξημένη ετοιμότητα ▌ του πλαισίου κυβερνοασφάλειας της Ένωσης. Η απειλή αυτή υπερβαίνει ***τον επιθετικό πόλεμο*** της Ρωσίας κατά της Ουκρανίας και είναι πιθανό να συνεχίσει να υφίσταται, δεδομένης της πληθώρας των ▌ παραγόντων ▌ που εμπλέκονται στις τρέχουσες γεωπολιτικές εντάσεις. Τέτοια περιστατικά μπορούν να παρεμποδίσουν την παροχή δημόσιων υπηρεσιών***, καθώς οι κυβερνοεπιθέσεις έχουν συχνά ως στόχο τοπικές, περιφερειακές ή εθνικές δημόσιες υπηρεσίες και υποδομές, ενώ οι τοπικές αρχές είναι ιδιαίτερα ευάλωτες, μεταξύ άλλων λόγω των περιορισμένων πόρων τους. Μπορούν επίσης να παρεμποδίσουν*** την άσκηση οικονομικών δραστηριοτήτων, μεταξύ άλλων σε τομείς ***υψηλής κρισιμότητας ή άλλους κρίσιμους τομείς***, να προκαλέσουν σημαντικές οικονομικές ζημίες, να υπονομεύσουν την εμπιστοσύνη των χρηστών, να προκαλέσουν σημαντική ζημία στην οικονομία ***και τα δημοκρατικά συστήματα*** 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 γρήγορα, δεν περιορίζονται σε κάποια συγκεκριμένη γεωγραφική περιοχή και συμβαίνουν ταυτόχρονα ή εξαπλώνονται αμέσως σε πολλές χώρες. ***Είναι σημαντικό να υπάρχει στενή συνεργασία μεταξύ του δημόσιου τομέα, του ιδιωτικού τομέα, της ακαδημαϊκής κοινότητας, της κοινωνίας των πολιτών και των μέσων ενημέρωσης.***

(3) Είναι απαραίτητο να ενισχυθεί η ανταγωνιστική θέση των τομέων της βιομηχανίας και των υπηρεσιών στην Ένωση σε ολόκληρη την ψηφιοποιημένη οικονομία και να στηριχθεί ο ψηφιακός μετασχηματισμός τους, διά της ενίσχυσης του επιπέδου κυβερνοασφάλειας στην ψηφιακή ενιαία αγορά***,*** όπως συνιστάται σε τρεις διαφορετικές προτάσεις της Διάσκεψης για το μέλλον της Ευρώπης***.*** Είναι αναγκαίο να αυξηθεί η ανθεκτικότητα των πολιτών, των επιχειρήσεων***, συμπεριλαμβανομένων των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων και των νεοφυών επιχειρήσεων,*** και των οντοτήτων που διαχειρίζονται κρίσιμες υποδομές***,*** έναντι των αυξανόμενων κυβερνοαπειλών, 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 ταχύτερη αντιμετώπιση κυβερνοαπειλών και περιστατικών κυβερνοασφάλειας. Επιπροσθέτως, τα κράτη μέλη χρειάζονται βοήθεια για την καλύτερη προετοιμασία για σημαντικά περιστατικά κυβερνοασφάλειας και περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας***, και την αντιμετώπισή τους, καθώς και βοήθεια κατά την αρχική ανάκαμψη από τα περιστατικά αυτά***. Η Ένωση θα πρέπει επίσης να αυξήσει τις ικανότητές της σε αυτούς τους τομείς, ιδίως όσον αφορά τη συλλογή και ανάλυση δεδομένων σχετικά με κυβερνοαπειλές και περιστατικά κυβερνοασφάλειας***, βασιζόμενη στις υφιστάμενες δομές και σε στενή συνεργασία με αυτές***.

(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, ιδίως με τον κανονισμό (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[5], τις οδηγίες 2013/40/ΕΕ[6] και (ΕΕ) 2022/2555[7] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και τη σύσταση (ΕΕ) 2017/1584 της Επιτροπής[8]. Επιπλέον, η σύσταση του Συμβουλίου της 8ης Δεκεμβρίου 2022 σχετικά με συντονισμένη προσέγγιση σε επίπεδο Ένωσης με σκοπό την ενίσχυση της ανθεκτικότητας των κρίσιμων υποδομών καλεί τα κράτη μέλη να λάβουν μέτρα και να συνεργαστούν 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 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).

6 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).

7 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).

8 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).

(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 την ενίσχυση της αλληλεγγύης σε επίπεδο Ένωσης για την καλύτερη ανίχνευση, προετοιμασία***, αντιμετώπιση και ανάκαμψη για κυβερνοαπειλές και περιστατικά κυβερνοασφάλειας, ιδίως με την ενίσχυση των ικανοτήτων υφιστάμενων δομών***. Επιπλέον, στο πλαίσιο των συμπερασμάτων του Συμβουλίου σχετικά με τη διαμόρφωση της στάσης της ΕΕ στον κυβερνοχώρο το Συμβούλιο κάλεσε την Επιτροπή να υποβάλει πρόταση σχετικά με ένα νέο ταμείο αντιμετώπισης καταστάσεων έκτακτης ανάγκης στον τομέα της κυβερνοασφάλειας.

(6) Η κοινή ανακοίνωση της Επιτροπής και του ύπατου εκπροσώπου της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας, της 10ης Νοεμβρίου 2022, που υποβλήθηκε στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο σχετικά με την πολιτική της ΕΕ για την κυβερνοάμυνα», ανήγγειλε μια πρωτοβουλία αλληλεγγύης της ΕΕ στον κυβερνοχώρο με στόχο την ενίσχυση των κοινών ικανοτήτων ανίχνευσης, την αντίληψη της κατάστασης και την αντίδραση της ΕΕ μέσω της προώθησης της ανάπτυξης υποδομής κέντρων επιχειρήσεων ασφάλειας της ΕΕ («SOC»), την στήριξη της σταδιακής δημιουργίας εφεδρείας στον τομέα της κυβερνοασφάλειας σε επίπεδο ΕΕ με υπηρεσίες από αξιόπιστους ιδιωτικούς παρόχους και την δοκιμή κρίσιμων οντοτήτων για πιθανά τρωτά σημεία με βάση εκτιμήσεις κινδύνου της ΕΕ.

(7) Είναι αναγκαίο να ενισχυθούν η ανίχνευση και η αντίληψη της κατάστασης όσον αφορά τις κυβερνοαπειλές και τα περιστατικά 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 περιστατικών κυβερνοασφάλειας και ***περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας***. ***Κατά συνέπεια, θα πρέπει να αναπτυχθεί πανευρωπαϊκό δίκτυο κυβερνοκόμβων («ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια») για τη δημιουργία συντονισμένων ικανοτήτων ανίχνευσης και αντίληψης της κατάστασης, για 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***, κατόπιν αιτήματός τους,*** όσον αφορά την προετοιμασία, την αντιμετώπιση, τον μετριασμό των επιπτώσεων και την ***αρχική*** ανάκαμψη από σημαντικά περιστατικά κυβερνοασφάλειας και περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας και για την υποστήριξη άλλων χρηστών για την αντιμετώπιση σημαντικών περιστατικών κυβερνοασφάλειας και περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας· και θα πρέπει να θεσπιστεί ευρωπαϊκός μηχανισμός εξέτασης περιστατικών κυβερνοασφάλειας για την εξέταση και την αξιολόγηση συγκεκριμένων σημαντικών περιστατικών κυβερνοασφάλειας ή περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας. ***Οι δράσεις στο πλαίσιο του παρόντος κανονισμού θα πρέπει να διεξάγονται με τον δέοντα σεβασμό προς τις αρμοδιότητες των κρατών μελών και θα πρέπει να συμπληρώνουν και να μην επικαλύπτουν τις δραστηριότητες που διεξάγονται από το δίκτυο CSIRT, το ευρωπαϊκό δίκτυο οργανισμών διασύνδεσης για τις κρίσεις στον κυβερνοχώρο (EU-CyCLONe) και την ομάδα συνεργασίας (ομάδα συνεργασίας NIS), που συστάθηκαν όλα δυνάμει της οδηγίας (ΕΕ) 2022/2555.*** Οι εν λόγω δράσεις δεν θίγουν τα άρθρα 107 και 108 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ).

(8) Για την επίτευξη των στόχων αυτών, είναι επίσης αναγκαίο να τροποποιηθεί ο κανονισμός (ΕΕ) 2021/694 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[9] 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 ***το ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια*** και τον μηχανισμό έκτακτης ανάγκης στον κυβερνοχώρο 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 κυβερνοαπειλών και στην αντιμετώπιση αυτών, καθώς και στην ενίσχυση της διασυνοριακής συνεργασίας ***και του διασυνοριακού συντονισμού*** στον τομέα της κυβερνοασφάλειας. ***Το ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια θα μπορούσε να διαδραματίσει σημαντικό ρόλο στη στήριξη των κρατών μελών όσον αφορά την πρόβλεψη κυβερνοαπειλών και την προστασία από αυτές, και η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας θα μπορούσε να διαδραματίσει σημαντικό ρόλο στη στήριξη των κρατών μελών, των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης και των τρίτων χωρών συνδεδεμένων με το*** πρόγραμμα «Ψηφιακή Ευρώπη» ***για την αντιμετώπιση και τον μετριασμό των επιπτώσεων σημαντικών περιστατικών κυβερνοασφάλειας, περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας και περιστατικών ισοδύναμων με περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας.***

[9] 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).

***Στις επιπτώσεις αυτές θα μπορούσαν να περιλαμβάνονται σημαντικές υλικές ή μη υλικές ζημίες και σοβαροί κίνδυνοι για τη δημόσια προστασία και ασφάλεια. Υπό το πρίσμα των ειδικών ρόλων που θα μπορούσαν να διαδραματίσουν το ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια και η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, με τον παρόντα κανονισμό θα πρέπει να τροποποιηθεί ο κανονισμός (ΕΕ) 2021/694 όσον αφορά τη συμμετοχή νομικών οντοτήτων που είναι εγκατεστημένες στην Ένωση αλλά ελέγχονται από τρίτες χώρες, όπου υπάρχει πραγματικός κίνδυνος να μην υπάρχουν στην Ένωση τα αναγκαία και επαρκή εργαλεία, υποδομές και υπηρεσίες, ή η αναγκαία και επαρκής τεχνολογία, εμπειρογνωσία και ικανότητα, και τα οφέλη της συμπερίληψης των οντοτήτων αυτών υπερτερούν του κινδύνου για την ασφάλεια. Θα πρέπει να θεσπιστούν οι*** ειδικές προϋποθέσεις υπό τις οποίες μπορεί να χορηγηθεί χρηματοδοτική στήριξη για ***δράσεις υλοποίησης του ευρωπαϊκού συστήματος προειδοποίησης για την κυβερνοασφάλεια και της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, και*** 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)*** ***Για να ενισχυθεί η αντίδραση της Ένωσης σε κυβερνοαπειλές και περιστατικά κυβερνοασφάλειας, είναι απολύτως απαραίτητο να υπάρχει συντονισμός με διεθνείς οργανισμούς καθώς και με αξιόπιστους και ομονοούντες διεθνείς εταίρους. Στο πλαίσιο αυτό, ως αξιόπιστοι και ομονοούντες διεθνείς εταίροι θα πρέπει να νοούνται οι χώρες που συμμερίζονται τις αρχές που ενέπνευσαν την δημιουργία της Ένωσης, ιδίως την δημοκρατία, το κράτος δικαίου, την οικουμενικότητα και το αδιαίρετο των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών, τον σεβασμό της ανθρώπινης αξιοπρέπειας, τις αρχές της ισότητας και της αλληλεγγύης, και τον σεβασμό των αρχών του Καταστατικού Χάρτη των Ηνωμένων Εθνών και του διεθνούς δικαίου, και οι οποίες δεν υπονομεύουν τα ουσιώδη συμφέροντα ασφάλειας της Ένωσης ή των κρατών μελών της.***

***Η συνεργασία αυτή θα μπορούσε επίσης να είναι επωφελής όσον αφορά τις δράσεις στο πλαίσιο του παρόντος κανονισμού, ιδίως σε σχέση με το ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια και την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας. Ο κανονισμός (ΕΕ) 2021/694 θα πρέπει να προβλέπει ότι, εάν πληρούνται ορισμένες προϋποθέσεις διαθεσιμότητας και ασφάλειας, οι προσκλήσεις υποβολής προσφορών για το ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια και την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας θα μπορούσαν να είναι ανοικτές σε νομικές οντότητες που ελέγχονται από τρίτες χώρες, με την επιφύλαξη των απαιτήσεων ασφάλειας. Όταν εξετάζεται εάν αυτό το άνοιγμα των δημοσίων συμβάσεων συνεπάγεται κίνδυνο για την ασφάλεια, είναι σημαντικό να λαμβάνονται υπόψη οι αρχές και οι αξίες που μοιράζεται η Ένωση με ομονοούντες διεθνείς εταίρους, στην περίπτωση που οι εν λόγω αρχές και αξίες σχετίζονται με ουσιώδη συμφέροντα ασφάλειας της Ένωσης. Επιπλέον, όταν εξετάζονται τέτοιες απαιτήσεις ασφάλειας βάσει του κανονισμού (ΕΕ) 2021/694, θα μπορούσαν να λαμβάνονται υπόψη διάφορα στοιχεία, όπως η εταιρική δομή και η διαδικασία λήψης αποφάσεων μιας οντότητας, η ασφάλεια των δεδομένων και των διαβαθμισμένων ή ευαίσθητων πληροφοριών, και η διασφάλιση ότι τα αποτελέσματα της δράσης δεν υπόκεινται σε έλεγχο ή περιορισμούς από μη επιλέξιμες τρίτες χώρες.***

(10) 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 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 τον κανονισμό (ΕΕ) 2021/694.

(11) 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) 2024/2509 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου***[10] και ρυθμίζουν ιδίως τις πρακτικές λεπτομέρειες κατάρτισης και εκτέλεσης του προϋπολογισμού της Ένωσης και οργανώνουν επίσης τον έλεγχο της ευθύνης των δημοσιονομικών φορέων. Οι κανόνες που θεσπίζονται βάσει του άρθρου 322 ΣΛΕΕ περιλαμβάνουν επίσης το γενικό καθεστώς αιρεσιμότητας για την προστασία του προϋπολογισμού της Ένωσης, όπως ορίζεται στον κανονισμό (ΕΕ, Ευρατόμ) 2020/2092 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[11].

---

10 ***Κανονισμός (ΕΕ, Ευρατόμ) 2024/2509 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Σεπτεμβρίου 2024, σχετικά με τους δημοσιονομικούς κανόνες που εφαρμόζονται στον γενικό προϋπολογισμό της Ένωσης (ΕΕ L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).***

11 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: http://data.europa.eu/eli/reg/2020/2092/oj).

***(12) Ενώ τα μέτρα πρόληψης και ετοιμότητας είναι απαραίτητα για την ενίσχυση της ανθεκτικότητας της Ένωσης στην αντιμετώπιση σημαντικών περιστατικών κυβερνοασφάλειας, περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας και περιστατικών ισοδύναμων με περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας, η εμφάνιση, η χρονική στιγμή και το μέγεθος των εν λόγω περιστατικών είναι εκ φύσεως απρόβλεπτα. Οι χρηματοδοτικοί πόροι που απαιτούνται για την εξασφάλιση επαρκούς αντιμετώπισης μπορεί να διαφέρουν σημαντικά από έτος σε έτος και θα πρέπει να μπορούν να διατίθενται αμέσως. Για να συμβιβαστεί η αρχή της προβλεψιμότητας του προϋπολογισμού με την αναγκαιότητα ταχείας αντίδρασης στις νέες ανάγκες απαιτείται συνεπώς η προσαρμογή της εκτέλεσης του προϋπολογισμού των προγραμμάτων εργασίας. Κατά συνέπεια, ενδείκνυται να εγκριθεί η μεταφορά αχρησιμοποίητων πιστώσεων, που θα περιορίζονται στο επόμενο έτος και θα προορίζονται αποκλειστικά για την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας και τις δράσεις στήριξης της αμοιβαίας συνδρομής, επιπλέον της μεταφοράς πιστώσεων βάσει του άρθρου 12 παράγραφος 4 του κανονισμού (ΕΕ, Ευρατόμ) 2024/2509.***

(13) 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 κυβερνοαπειλών περιλαμβάνει αυξημένη ικανότητα προηγμένων δυνατοτήτων ανίχνευσης. Το ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια θα πρέπει να αποτελείται από διάφορους διαλειτουργικούς διασυνοριακούς κυβερνοκόμβους, καθένας από τους οποίους συγκεντρώνει τρεις ή περισσότερους εθνικούς κυβερνοκόμβους.*** Οι εν λόγω υποδομές θα πρέπει να εξυπηρετούν εθνικά και ενωσιακά συμφέροντα και ανάγκες κυβερνοασφάλειας, αξιοποιώντας την τεχνολογία αιχμής για προηγμένα εργαλεία συλλογής σχετικών δεδομένων και πληροφοριών, ***ανωνυμοποιημένων κατά περίπτωση,*** και εργαλεία ανάλυσης, ενισχύοντας τις ***συντονισμένες*** ικανότητες ανίχνευσης και διαχείρισης στον κυβερνοχώρο και παρέχοντας αντίληψη της κατάστασης σε πραγματικό χρόνο. Οι υποδομές αυτές θα πρέπει να χρησιμεύουν για ***τη βελτίωση της κατάστασης κυβερνοασφάλειας, με την ενίσχυση της ανίχνευσης, της συγκέντρωσης και της ανάλυσης δεδομένων και πληροφοριών με στόχο την πρόληψη κυβερνο***απειλών και περιστατικών 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 EU-CyCLONe ▌.

(14) ***Η συμμετοχή στο ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια είναι προαιρετική για τα κράτη μέλη.*** Κάθε κράτος μέλος θα πρέπει να ορίσει ***μία ενιαία οντότητα*** σε εθνικό επίπεδο ***επιφορτισμένη*** με τον συντονισμό των δραστηριοτήτων ανίχνευσης κυβερνοαπειλών στο εν λόγω κράτος μέλος. ***Οι εν λόγω εθνικοί κυβερνοκόμβοι*** θα πρέπει να λειτουργούν ως σημείο αναφοράς και πύλη σε εθνικό επίπεδο για τη συμμετοχή ***στο ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια*** και θα πρέπει να διασφαλίζουν ότι οι πληροφορίες για τις κυβερνοαπειλές από δημόσιες και ιδιωτικές οντότητες ανταλλάσσονται και συλλέγονται σε εθνικό επίπεδο με αποτελεσματικό και εξορθολογισμένο τρόπο. ***Οι εθνικοί κυβερνοκόμβοι θα μπορούσαν να ενισχύσουν τη συνεργασία και την ανταλλαγή πληροφοριών μεταξύ δημόσιων και ιδιωτικών οντοτήτων και θα μπορούσαν επίσης να στηρίξουν την ανταλλαγή σχετικών δεδομένων και πληροφοριών με σχετικές τομεακές και διατομεακές κοινότητες, συμπεριλαμβανομένων των σχετικών κέντρων ανταλλαγής και ανάλυσης πληροφοριών του κλάδου (ΚΑΑΠ). Η στενή και συντονισμένη συνεργασία μεταξύ δημόσιων και ιδιωτικών οντοτήτων είναι πολύ σημαντική για την ενίσχυση της κυβερνοανθεκτικότητας της Ένωσης. Η εν λόγω συνεργασία αποτελεί ιδιαίτερα πολύτιμο στοιχείο στο πλαίσιο της ανταλλαγής πληροφοριών για τις κυβερνοαπειλές με σκοπό τη βελτίωση της ενεργητικής κυβερνοπροστασίας. Στο πλαίσιο αυτής της συνεργασίας και ανταλλαγής πληροφοριών, οι εθνικοί κυβερνοκόμβοι θα μπορούσαν να ζητούν και να λαμβάνουν συγκεκριμένες πληροφορίες.***

***Οι εν λόγω εθνικοί κυβερνοκόμβοι δεν υποχρεούνται από τον παρόντα κανονισμό να εκτελούν τα αιτήματα αυτά, ούτε και εξουσιοδοτούνται να επιβάλλουν την εκτέλεσή τους. Κατά περίπτωση και σύμφωνα με το ενωσιακό και το εθνικό δίκαιο, οι πληροφορίες που ζητούνται ή λαμβάνονται θα μπορούσαν να περιλαμβάνουν δεδομένα τηλεμετρίας, αισθητήρων και καταγραφής από οντότητες, όπως παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας, που δραστηριοποιούνται σε τομείς υψηλής κρισιμότητας ή άλλους κρίσιμους τομείς εντός του εν λόγω κράτους μέλους, προκειμένου να ενισχυθεί ο ταχύς εντοπισμός δυνητικών κυβερνοαπειλών και περιστατικών σε προγενέστερο στάδιο, και με τον τρόπο αυτό να βελτιωθεί η αντίληψη της κατάστασης. Εάν ο εθνικός κυβερνοκόμβος δεν είναι η αρμόδια αρχή που έχει οριστεί ή συσταθεί από το οικείο κράτος μέλος δυνάμει του άρθρου 8 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555, είναι ζωτικής σημασίας ο κόμβος αυτός να συντονίζεται με την εν λόγω αρμόδια αρχή όσον αφορά αυτά τα αιτήματα παροχής δεδομένων και την παραλαβή εν λόγω δεδομένων.***

(15) Στο πλαίσιο ***του ευρωπαϊκού συστήματος προειδοποίησης για την κυβερνοασφάλεια***, θα πρέπει να δημιουργηθούν ***ορισμένοι διασυνοριακοί κυβερνοκόμβοι***. Σε ***αυτούς*** τους διασυνοριακούς κυβερνοκόμβους θα πρέπει να συμμετέχουν ***εθνικοί κυβερνοκόμβοι*** 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 ***κυβερνοκόμβων*** θα πρέπει να είναι η ενίσχυση των ικανοτήτων ανάλυσης, πρόληψης και ανίχνευσης κυβερνοαπειλών και η υποστήριξη της παραγωγής υψηλής ποιότητας πληροφοριών για τις κυβερνοαπειλές, ιδίως μέσω της ανταλλαγής ***σχετικών πληροφοριών, ανωνυμοποιημένων κατά περίπτωση, σε ένα αξιόπιστο και ασφαλές περιβάλλον,*** 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. Οι διασυνοριακοί κυβερνοκόμβοι θα πρέπει να παρέχουν νέα πρόσθετη ικανότητα, αξιοποιώντας και συμπληρώνοντας τα υφιστάμενα SOC και τις υφιστάμενες ▌CSIRT▌ και άλλους σχετικούς παράγοντες***, συμπεριλαμβανομένου του δικτύου CSIRT***.

***(16)*** ***Ένα κράτος μέλος που επιλέγεται από το Ευρωπαϊκό Κέντρο Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας (ΕΚΑΚ) που θεσπίστηκε με τον κανονισμό (ΕΕ) 2021/887 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[12] κατόπιν πρόσκλησης εκδήλωσης ενδιαφέροντος για τη δημιουργία, ή ενίσχυση των ικανοτήτων, εθνικού κυβερνοκόμβου, θα πρέπει από κοινού με το ΕΚΑΚ να αγοράζει σχετικά εργαλεία, υποδομές ή υπηρεσίες. Το εν λόγω κράτος μέλος θα πρέπει να είναι επιλέξιμο να λάβει επιχορήγηση για τη λειτουργία των εργαλείων, των υποδομών ή των υπηρεσιών. Μια κοινοπραξία υποδοχής αποτελούμενη από τουλάχιστον τρία κράτη μέλη, η οποία έχει επιλεγεί από το ΕΚΑΚ κατόπιν πρόσκλησης εκδήλωσης ενδιαφέροντος για τη δημιουργία ή την ενίσχυση των ικανοτήτων διασυνοριακού κυβερνοκόμβου, θα πρέπει να αγοράζει σχετικά εργαλεία, υποδομές ή υπηρεσίες από κοινού με το ΕΚΑΚ. Η κοινοπραξία υποδοχής θα πρέπει να είναι επιλέξιμη να λάβει επιχορήγηση για τη λειτουργία των εργαλείων, των υποδομών ή των υπηρεσιών. Η διαδικασία προμήθειας για την αγορά των σχετικών εργαλείων, υποδομών ή υπηρεσιών θα πρέπει να διεξάγεται από κοινού από το ΕΚΑΚ και τις αρμόδιες αναθέτουσες αρχές των κρατών μελών που επιλέγονται κατόπιν των εν λόγω προσκλήσεων εκδήλωσης ενδιαφέροντος.***

---

[12] ***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: http://data.europa.eu/eli/reg/2021/887/oj).***

***Η εν λόγω προμήθεια θα πρέπει να είναι σύμφωνη με το άρθρο 168 παράγραφος 2 του κανονισμού (ΕΕ, Ευρατόμ) 2024/2509 και με τους δημοσιονομικούς κανόνες του ΕΚΑΚ. Κατά συνέπεια, οι ιδιωτικές οντότητες δεν θα πρέπει να είναι επιλέξιμες για συμμετοχή στις προσκλήσεις εκδήλωσης ενδιαφέροντος για την από κοινού αγορά εργαλείων, υποδομών ή υπηρεσιών με το ΕΚΑΚ, ή για τη λήψη επιχορηγήσεων για τη λειτουργία των εν λόγω εργαλείων, υποδομών ή υπηρεσιών. Ωστόσο, τα κράτη μέλη θα πρέπει να έχουν τη δυνατότητα να συμπεριλαμβάνουν ιδιωτικές οντότητες στη δημιουργία, την ενίσχυση και τη λειτουργία των εθνικών κυβερνοκόμβων τους και των διασυνοριακών κυβερνοκόμβων με άλλους τρόπους που κρίνουν κατάλληλους, σύμφωνα με το ενωσιακό και το εθνικό δίκαιο. Οι ιδιωτικές οντότητες θα μπορούσαν επίσης να είναι επιλέξιμες για χρηματοδότηση από την Ένωση σύμφωνα με τον κανονισμό (ΕΕ) 2021/887 για τον σκοπό της παροχής στήριξης σε εθνικούς κυβερνοκόμβους.***

***(17) Προκειμένου να ενισχυθεί η ανίχνευση κυβερνοαπειλών και η αντίληψη της κατάστασης στην Ένωση, ένα κράτος μέλος που επιλέγεται κατόπιν πρόσκλησης εκδήλωσης ενδιαφέροντος για τη δημιουργία ή την ενίσχυση των ικανοτήτων εθνικού κυβερνοκόμβου, θα πρέπει να δεσμευτεί να υποβάλει αίτηση συμμετοχής σε διασυνοριακό κυβερνοκόμβο. Εάν ένα κράτος μέλος δεν συμμετέχει σε διασυνοριακό κυβερνοκόμβο εντός δύο ετών από την ημερομηνία κατά την οποία αποκτώνται τα εργαλεία, οι υποδομές ή οι υπηρεσίες ή κατά την οποία λαμβάνει χρηματοδότηση μέσω επιχορηγήσεων, όποιο από τα δύο συμβεί νωρίτερα, δεν θα πρέπει να είναι επιλέξιμο να συμμετάσχει σε περαιτέρω ενωσιακές δράσεις στήριξης εντός του πλαισίου του ευρωπαϊκού συστήματος προειδοποίησης για την κυβερνοασφάλεια για την ενίσχυση των ικανοτήτων του εθνικού κυβερνοκόμβου του. Στις περιπτώσεις αυτές, οντότητες από τα κράτη μέλη θα μπορούσαν να συνεχίσουν να συμμετέχουν σε προσκλήσεις υποβολής προτάσεων για άλλα θέματα στο πλαίσιο του προγράμματος «Ψηφιακή Ευρώπη» ή άλλων ενωσιακών χρηματοδοτικών προγραμμάτων, συμπεριλαμβανομένων προσκλήσεων υποβολής προτάσεων για ικανότητες ανίχνευσης κυβερνοαπειλών και ανταλλαγής πληροφοριών, υπό την προϋπόθεση ότι οι εν λόγω οντότητες πληρούν τα κριτήρια επιλεξιμότητας που καθορίζονται στα προγράμματα αυτά.***

(18) ▌Οι CSIRT ανταλλάσσουν πληροφορίες στο πλαίσιο του δικτύου CSIRT, σύμφωνα με την οδηγία (ΕΕ) 2022/2555. ***Το ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια θα πρέπει να αποτελέσει μια νέα ικανότητα που θα συμπληρώνει το δίκτυο CSIRT, συμβάλλοντας στη δημιουργία μιας ενωσιακής αντίληψης της κατάστασης που θα επιτρέπει την ενίσχυση των ικανοτήτων του δικτύου CSIRT. Οι διασυνοριακοί κυβερνοκόμβοι θα πρέπει να συντονίζονται και να συνεργάζονται στενά με το δίκτυο CSIRT. Θα πρέπει να ενεργούν συγκεντρώνοντας δεδομένα και ανταλλάσσοντας συναφείς πληροφορίες, ανωνυμοποιημένες κατά περίπτωση, που αφορούν κυβερνοαπειλές από δημόσιες και ιδιωτικές οντότητες, ενισχύοντας την αξία των εν λόγω δεδομένων και πληροφοριών 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, καθώς και στην ανάπτυξη των ικανοτήτων της Ένωσης.***

(19) ***Οι διασυνοριακοί κυβερνοκόμβοι*** θα πρέπει να ***λειτουργούν*** ως κεντρικά σημεία που επιτρέπουν την ευρεία συγκέντρωση σχετικών δεδομένων και πληροφοριών για κυβερνοαπειλές, και να ***καθιστούν*** δυνατή τη διάδοση πληροφοριών σχετικά με απειλές σε ένα ευρύ και ποικίλο σύνολο ***ενδιαφερόμενων μερών, όπως*** τις ομάδες αντιμετώπισης καταστάσεων έκτακτης ανάγκης σε υπολογιστές (CERT), τις CSIRT, τα ΚΑΑΠ και τους φορείς εκμετάλλευσης κρίσιμων υποδομών. ***Τα μέλη της κοινοπραξίας υποδοχής θα πρέπει να προσδιορίζουν στη συμφωνία κοινοπραξίας τις σχετικές πληροφορίες που πρέπει να ανταλλάσσονται μεταξύ των συμμετεχόντων στον οικείο διασυνοριακό κυβερνοκόμβο.*** Οι πληροφορίες που ανταλλάσσονται μεταξύ των συμμετεχόντων σε διασυνοριακό ***κυβερνοκόμβο*** θα μπορούσαν να περιλαμβάνουν***, για παράδειγμα,*** δεδομένα από δίκτυα και αισθητήρες, ροές πληροφοριών σχετικά με απειλές, ενδείξεις παραβίασης, και πλαισιωμένες πληροφορίες σχετικά με περιστατικά, κυβερνοαπειλές**,** παρ' ολίγον περιστατικά, ***ευπάθειες, τεχνικές και διαδικασίες, εχθρικές τακτικές, πληροφορίες που αφορούν συγκεκριμένους παράγοντες απειλής, προειδοποιήσεις για την κυβερνοασφάλεια και συστάσεις σχετικά με την παραμετροποίηση εργαλείων κυβερνοασφάλειας για τον εντοπισμό κυβερνοεπιθέσεων***. Επιπλέον, ***οι διασυνοριακοί κυβερνοκόμβοι*** θα πρέπει επίσης να συνάπτουν συμφωνίες συνεργασίας μεταξύ τους.

***Οι εν λόγω συμφωνίες συνεργασίας θα πρέπει, ειδικότερα, να προσδιορίζουν τις αρχές ανταλλαγής πληροφοριών και τη διαλειτουργικότητα. Οι ρήτρες τους σχετικά με τη διαλειτουργικότητα, και συγκεκριμένα όσον αφορά τους μορφότυπους και τα πρωτόκολλα ανταλλαγής πληροφοριών, θα πρέπει να έχουν ως σημείο αναφοράς και αφετηρία τις κατευθυντήριες γραμμές διαλειτουργικότητας που εκδίδει ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια που θεσπίστηκε με τον κανονισμό (ΕΕ) 2019/881 (ENISA). Οι εν λόγω κατευθυντήριες γραμμές θα πρέπει να εκδίδονται ταχέως, ώστε να διασφαλίζεται ότι μπορούν να λαμβάνονται υπόψη από τους διασυνοριακούς κυβερνοκόμβους σε πρώιμο στάδιο. Θα πρέπει να λαμβάνουν υπόψη τα διεθνή πρότυπα και τις βέλτιστες πρακτικές, και την λειτουργία διασυνοριακών κυβερνοκόμβων που έχουν συσταθεί.***

***(20) Οι διασυνοριακοί κυβερνοκόμβοι και το δίκτυο CSIRT θα πρέπει να συνεργάζονται στενά προκειμένου να διασφαλίζουν τις συνέργειες και τη συμπληρωματικότητα των δραστηριοτήτων. Για τον σκοπό αυτό, θα πρέπει να καταλήγουν σε συμφωνία όσον αφορά τις διαδικαστικές ρυθμίσεις για τη συνεργασία και την ανταλλαγή σχετικών πληροφοριών. Αυτό θα μπορούσε να περιλαμβάνει την ανταλλαγή σχετικών πληροφοριών για κυβερνοαπειλές και σημαντικά περιστατικά κυβερνοασφάλειας και τη διασφάλιση ότι η εμπειρία από προηγμένα εργαλεία, ιδίως εργαλεία τεχνητής νοημοσύνης και τεχνολογίας ανάλυσης δεδομένων, που χρησιμοποιήθηκαν στο πλαίσιο των διασυνοριακών κυβερνοκόμβων, διαμοιράζεται στο δίκτυο CSIRT.***

(21) Η κοινή αντίληψη της κατάστασης μεταξύ των αρμόδιων αρχών αποτελεί απαραίτητη προϋπόθεση για την ετοιμότητα και τον συντονισμό σε επίπεδο Ένωσης όσον αφορά σημαντικά περιστατικά κυβερνοασφάλειας και περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας. Με την οδηγία (ΕΕ) 2022/2555 συγκροτήθηκε το EU-CyCLONe προκειμένου 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. ***Με την οδηγία (ΕΕ) 2022/2555 συγκροτήθηκε επίσης το δίκτυο CSIRT για την προώθηση της ταχείας και αποτελεσματικής επιχειρησιακής συνεργασίας μεταξύ όλων των κρατών μελών. Για να διασφαλίζεται η αντίληψη της κατάστασης και να ενισχύεται η αλληλεγγύη, σε περιπτώσεις όπου οι διασυνοριακοί κυβερνοκόμβοι λαμβάνουν πληροφορίες σχετικά με πιθανό ή εξελισσόμενο περιστατικό μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας, θα πρέπει να παρέχουν σχετικές πληροφορίες στο δίκτυο CSIRT και να ενημερώνουν, υπό μορφή έγκαιρης προειδοποίησης, το EU-CyCLONe. 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 περιστατικό μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας. Στο πλαίσιο αυτό, θα πρέπει να λαμβάνεται δεόντως υπόψη η αρχή της ανάγκης για γνώση και ο δυνητικά ευαίσθητος χαρακτήρας των πληροφοριών που ανταλλάσσονται.***

Η οδηγία (ΕΕ) 2022/2555 υπενθυμίζει επίσης τις αρμοδιότητες της Επιτροπής στο πλαίσιο του μηχανισμού πολιτικής προστασίας της Ένωσης (ΜΠΠΕ) που θεσπίστηκε με την απόφαση αριθ. 1313/2013/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[13], και την αρμοδιότητά της όσον αφορά την υποβολή αναλυτικών εκθέσεων για τις ρυθμίσεις για την ολοκληρωμένη αντιμετώπιση πολιτικών κρίσεων της ΕΕ (ρυθμίσεις IPCR) δυνάμει της εκτελεστικής απόφασης (ΕΕ) 2018/1993 του Συμβουλίου[14]. ***Όταν οι διασυνοριακοί κυβερνοκόμβοι διαμοιράζουν στο EU-CyCLONe και στο δίκτυο CSIRT σχετικές πληροφορίες και έγκαιρες προειδοποιήσεις που σχετίζονται με δυνητικό ή εν εξελίξει περιστατικό κυβερνοασφάλειας μεγάλης κλίμακας, είναι επιτακτική ανάγκη οι πληροφορίες αυτές να διαμοιράζονται μέσω των εν λόγω δικτύων στις αρχές των κρατών μελών, καθώς και στην Επιτροπή. Στο πλαίσιο αυτό, η οδηγία (ΕΕ) 2022/2555 προβλέπει ότι το EU-CyCLONe έχει ως σκοπό να στηρίζει τη συντονισμένη διαχείριση περιστατικών και κρίσεων μεγάλης κλίμακας 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. Στα καθήκοντα του EU-CyCLONe περιλαμβάνεται η ανάπτυξη κοινής αντίληψης της κατάστασης για τέτοια περιστατικά και κρίσεις. Είναι υψίστης σημασίας το EU-CyCLONe να διασφαλίζει, σύμφωνα με τον εν λόγω σκοπό και τα καθήκοντά του, ότι οι εν λόγω πληροφορίες υποβάλλονται άμεσα στους σχετικούς εκπροσώπους των κρατών μελών και στην Επιτροπή. Για τον σκοπό αυτό, είναι ιδιαίτερα σημαντικό να συμπεριληφθούν κατάλληλες διατάξεις στον εσωτερικό κανονισμό του EU-CyCLONe.***

---

13 ***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, ELI: http://data.europa.eu/eli/dec/2013/1313/oj).***

14 ***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: http://data.europa.eu/eli/dec_impl/2018/1993/oj).***

(22) Οι οντότητες που συμμετέχουν ***στο ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια*** 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. Θα πρέπει να διασφαλίζουν επίσης 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 ***των αιτίων των εντοπιζόμενων κυβερνοαπειλών και κινδύνων,*** θα πρέπει να λαμβάνουν υπόψη ***το υφιστάμενο έργο που έχει πραγματοποιηθεί*** στο πλαίσιο της εφαρμογής της οδηγίας (ΕΕ) 2022/2555.

(23) Προκειμένου να καταστεί δυνατή η ανταλλαγή ***σχετικών*** δεδομένων ***και πληροφοριών όσον αφορά*** κυβερνοαπειλές από διάφορες πηγές, σε ευρεία κλίμακα και σε ένα αξιόπιστο ***και ασφαλές*** περιβάλλον, οι οντότητες που συμμετέχουν ***στο ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια*** θα πρέπει να είναι εφοδιασμένες με προηγμένα, υψηλής ασφάλειας εργαλεία, εξοπλισμό και υποδομές***, καθώς και με 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.

(24) Με τη συλλογή, ***την ανάλυση,*** τον διαμοιρασμό και την ανταλλαγή ***σχετικών δεδομένων και πληροφοριών***, ***το ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια*** θα πρέπει να ενισχύσει την τεχνολογική κυριαρχία της Ένωσης ***και την ανοικτή στρατηγική αυτονομία στον τομέα της κυβερνοασφάλειας, την ανταγωνιστικότητα και την ανθεκτικότητα***. Η συγκέντρωση επιμελημένων δεδομένων υψηλής ποιότητας θα ***μπορούσε*** επίσης να συμβάλει στην ανάπτυξη προηγμένων τεχνολογιών τεχνητής νοημοσύνης και ανάλυσης δεδομένων. ***Η ύπαρξη ανθρώπινης εποπτείας και, ως εκ τούτου, ειδικευμένου εργατικού δυναμικού παραμένει ουσιαστική για την αποτελεσματική συγκέντρωση δεδομένων υψηλής ποιότητας.***

(25) Ενώ ***το ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια*** 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. ▌

(26) Η ανταλλαγή πληροφοριών μεταξύ των συμμετεχόντων ***στο ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια*** 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 την οντότητα που καθιστά τα δεδομένα διαθέσιμα ότι τα δεδομένα έχουν καταστραφεί.

*(27)* ***Η διαφύλαξη της εμπιστευτικότητας και της ασφάλειας των πληροφοριών είναι υψίστης σημασίας και για τους τρεις πυλώνες του παρόντος κανονισμού, και συγκεκριμένα προκειμένου να ενθαρρύνεται ο διαμοιρασμός ή η ανταλλαγή πληροφοριών στο πλαίσιο του ευρωπαϊκού συστήματος προειδοποίησης για την κυβερνοασφάλεια, να διαφυλάσσονται τα συμφέροντα των οντοτήτων που υποβάλλουν αίτηση στήριξης στο πλαίσιο του μηχανισμού έκτακτης ανάγκης για την κυβερνοασφάλεια, και να διασφαλίζεται ότι οι εκθέσεις στο πλαίσιο του ευρωπαϊκού μηχανισμού εξέτασης περιστατικών κυβερνοασφάλειας μπορούν να αποφέρουν χρήσιμα διδάγματα χωρίς αρνητικό αντίκτυπο στις οντότητες που επηρεάζονται από τα περιστατικά. Η συμμετοχή των κρατών μελών και των οντοτήτων στους μηχανισμούς αυτούς εξαρτάται από τις σχέσεις εμπιστοσύνης μεταξύ των συνιστωσών τους. Όταν οι πληροφορίες είναι εμπιστευτικές σύμφωνα με ενωσιακούς ή εθνικούς κανόνες, ο διαμοιρασμός ή η ανταλλαγή τους δυνάμει του παρόντος κανονισμού θα πρέπει να περιορίζεται σε ό,τι είναι συναφές και αναλογικό προς τον σκοπό του διαμοιρασμού ή της ανταλλαγής. Ο εν λόγω διαμοιρασμός ή ανταλλαγή θα πρέπει επίσης να διαφυλάσσει την εμπιστευτικότητα των πληροφοριών αυτών, μεταξύ άλλων με την προστασία των συμφερόντων ασφάλειας και των εμπορικών συμφερόντων των οικείων οντοτήτων. Ο διαμοιρασμός ή η ανταλλαγή πληροφοριών δυνάμει του παρόντος κανονισμού θα μπορούσε να πραγματοποιείται με τη χρήση συμφωνιών τήρησης του απορρήτου ή κατευθυντήριων γραμμών σχετικά με τη διανομή πληροφοριών, όπως το πρωτόκολλο φωτεινού σηματοδότη (TLP). Το TLP πρέπει να νοείται ως μέσο που επιτρέπει την παροχή πληροφοριών σχετικά με τυχόν περιορισμούς στην περαιτέρω διάδοση πληροφοριών. Χρησιμοποιείται σε όλες σχεδόν τις CSIRT και σε ορισμένα ΚΑΑΠ. Εκτός από αυτές τις γενικές απαιτήσεις, όσον αφορά το ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια, οι συμφωνίες κοινοπραξιών υποδοχής θα πρέπει να θεσπίζουν ειδικούς κανόνες σχετικά με τους όρους ανταλλαγής πληροφοριών εντός του οικείου διασυνοριακού κυβερνοκόμβου. Οι συμφωνίες αυτές θα μπορούσαν, ειδικότερα, να προβλέπουν ότι η ανταλλαγή πληροφοριών πρέπει να πραγματοποιείται μόνο σύμφωνα με το ενωσιακό και το εθνικό δίκαιο.***

***(28) Όσον αφορά την ανάπτυξη της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, απαιτούνται ειδικοί κανόνες εμπιστευτικότητας. Η στήριξη θα ζητείται, θα αξιολογείται και θα παρέχεται σε συνθήκες κρίσης και σε σχέση με οντότητες που δραστηριοποιούνται σε ευαίσθητους τομείς. Για την αποτελεσματική λειτουργία της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, είναι σημαντικό οι χρήστες και οι οντότητες να είναι σε θέση να ανταλλάσσουν και να παρέχουν πρόσβαση, χωρίς καθυστέρηση, σε όλες τις πληροφορίες που είναι απαραίτητες ώστε κάθε οντότητα να συμβάλει στην αξιολόγηση των αιτημάτων και την παροχή στήριξης. Κατά συνέπεια, ο παρών κανονισμός θα πρέπει να προβλέπει ότι όλες αυτές οι πληροφορίες χρησιμοποιούνται ή ανταλλάσσονται μόνο όταν αυτό είναι αναγκαίο για τη λειτουργία της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, και ότι οι πληροφορίες που είναι εμπιστευτικές ή διαβαθμισμένες σύμφωνα με το ενωσιακό και το εθνικό δίκαιο θα πρέπει να χρησιμοποιούνται και να ανταλλάσσονται μόνο σύμφωνα με το εν λόγω δίκαιο. Επιπλέον, οι χρήστες θα πρέπει να είναι σε θέση, κατά περίπτωση, να χρησιμοποιούν πρωτόκολλα ανταλλαγής πληροφοριών, όπως το TLP, για τον περαιτέρω καθορισμό περιορισμών. Ενώ οι χρήστες έχουν διακριτική ευχέρεια στο θέμα αυτό, είναι σημαντικό, κατά την εφαρμογή τέτοιων περιορισμών, να λαμβάνουν υπόψη τις πιθανές συνέπειες, ιδίως όσον αφορά την καθυστέρηση της αξιολόγησης ή της παράδοσης των ζητούμενων υπηρεσιών. Προκειμένου να είναι αποτελεσματική η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, είναι σημαντικό η αναθέτουσα αρχή να αποσαφηνίζει τις συνέπειες αυτές στον χρήστη πριν από την υποβολή αιτήματος. Οι εν λόγω διασφαλίσεις περιορίζονται στο αίτημα και την παροχή υπηρεσιών από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας και δεν επηρεάζουν την ανταλλαγή πληροφοριών υπό άλλες συνθήκες, όπως σε σχέση με τις διαδικασίες προμήθειας της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας.***

I

(29) Λαμβανομένων υπόψη των αυξανόμενων κινδύνων και του αριθμού των περιστατικών που επηρεάζουν τα κράτη μέλη, είναι αναγκαίο να δημιουργηθεί ένα μέσο στήριξης κρίσεων***, και συγκεκριμένα ο μηχανισμός έκτακτης ανάγκης για την κυβερνοασφάλεια,*** για τη βελτίωση της ανθεκτικότητας της Ένωσης σε σημαντικά περιστατικά κυβερνοασφάλειας, περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας, και περιστατικά ισοδύναμα με περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας, και για τη συμπλήρωση των δράσεων των κρατών μελών μέσω χρηματοδοτικής στήριξης έκτακτης ανάγκης για ετοιμότητα, αντιμετώπιση περιστατικών και ***αρχική*** ανάκαμψη της λειτουργίας βασικών υπηρεσιών. ***Δεδομένου ότι η πλήρης ανάκαμψη από περιστατικό αποτελεί ολοκληρωμένη διαδικασία επαναφοράς της λειτουργίας της επηρεαζόμενης οντότητας στην προ του περιστατικού κατάσταση, η οποία θα μπορούσε να αποβεί μακροχρόνια και να συνεπάγεται σημαντικό κόστος, η στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας θα πρέπει να περιορίζεται στο αρχικό στάδιο της διαδικασίας ανάκαμψης, που οδηγεί στην αποκατάσταση των βασικών λειτουργιών των συστημάτων.*** Ο μηχανισμός έκτακτης ανάγκης για την κυβερνοασφάλεια 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 (ΣΕΕ).

(30) 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 περιστατικών κυβερνοασφάλειας και περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας και ***αρχικής*** ανάκαμψης από αυτά, όπως οι υπηρεσίες που παρέχονται από τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (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 συμπεριλαμβανομένων, στο πλαίσιο του άρθρου 42 παράγραφος 7 ΣΕΕ, και των ομάδων ταχείας αντίδρασης στον κυβερνοχώρο ▌στο πλαίσιο της μόνιμης διαρθρωμένης συνεργασίας (PESCO) που θεσπίστηκαν δυνάμει της απόφασης (ΚΕΠΠΑ) 2017/2315 του Συμβουλίου[15]. Θα πρέπει να αντιμετωπίσει την ανάγκη να διασφαλιστεί η διαθεσιμότητα εξειδικευμένων μέσων για τη στήριξη της ετοιμότητας***, της αντιμετώπισης και της ανάκαμψης από τα περιστατικά αυτά, σε ολόκληρη την Ένωση και σε τρίτες χώρες συνδεδεμένες με το*** πρόγραμμα «Ψηφιακή Ευρώπη».

---

**15** 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 (ΕΕ L 331 της 14.12.2017, σ. 57, ELI: http://data.europa.eu/eli/dec/2017/2315/2023-05-23).

(31) Ο παρών κανονισμός δεν θίγει τις διαδικασίες και τα πλαίσια για τον συντονισμό της αντιμετώπισης κρίσεων σε επίπεδο Ένωσης, ιδίως την οδηγία (ΕΕ) 2022/2555, ***τον μηχανισμό πολιτικής προστασίας της Ένωσης που θεσπίστηκε με την απόφαση αριθ. 1313/2013/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[16], τις ρυθμίσεις IPCR και τη σύσταση (ΕΕ) 2017/1584 της Επιτροπής[17]. Η στήριξη που παρέχεται 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, λαμβανομένου υπόψη του μη στρατιωτικού χαρακτήρα του μηχανισμού έκτακτης ανάγκης για την κυβερνοασφάλεια. Η στήριξη που παρέχεται στο πλαίσιο του μηχανισμού έκτακτης ανάγκης για την κυβερνοασφάλεια μπορεί να συμπληρώνει δράσεις που υλοποιούνται στο πλαίσιο του άρθρου 42 παράγραφος 7 ΣΕΕ, συμπεριλαμβανομένης της βοήθειας που παρέχεται από ένα κράτος μέλος σε άλλο, ή να αποτελεί μέρος της κοινής αντίδρασης της Ένωσης και των κρατών μελών, ή να συμπληρώνει δράσεις που υλοποιούνται σε καταστάσεις που αναφέρονται στο άρθρο 222 ΣΛΕΕ. Η εφαρμογή του παρόντος κανονισμού*** θα πρέπει επίσης να συντονίζεται με την εφαρμογή των μέτρων ***στο πλαίσιο*** της εργαλειοθήκης για τη διπλωματία στον κυβερνοχώρο ▌, κατά περίπτωση.

---

16 ***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).***

17 ***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).***

***(32)*** 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, των κρατών μελών και, κατά περίπτωση, του ΕΚΑΚ***. 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.

(33) 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 περιστατικών κυβερνοασφάλειας και περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας, τη στήριξη της ***αρχικής*** ανάκαμψης ***ή*** την αποκατάσταση ***των βασικών λειτουργιών των υπηρεσιών που παρέχονται από οντότητες που δραστηριοποιούνται σε τομείς υψηλής κρισιμότητας ή οντοτήτων που δραστηριοποιούνται σε άλλους κρίσιμους τομείς***.

(34) 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 ***υψηλής κρισιμότητας*** οι οποίοι προσδιορίζονται σύμφωνα με την οδηγία (ΕΕ) 2022/2555 με συντονισμένο τρόπο***, μεταξύ άλλων μέσω ασκήσεων και εκπαίδευσης***. Για τον σκοπό αυτό, η Επιτροπή, ***κατόπιν διαβούλευσης με τον*** ENISA***, η*** ομάδα συνεργασίας NIS ***και το EU-CyCLONe***, θα πρέπει να ***προσδιορίζουν*** τακτικά σχετικούς τομείς ή υποτομείς, οι οποίοι θα πρέπει να είναι επιλέξιμοι για χρηματοδοτική στήριξη για συντονισμένες δοκιμές ετοιμότητας σε επίπεδο Ένωσης. Οι τομείς ή υποτομείς θα πρέπει να επιλέγονται από τους τομείς υψηλής κρισιμότητας του παραρτήματος Ι της οδηγίας (ΕΕ) 2022/2555. Οι συντονισμένες δοκιμές ετοιμότητας θα πρέπει να βασίζονται σε κοινά σενάρια και μεθοδολογίες κινδύνου. Κατά την επιλογή των τομέων και την ανάπτυξη σεναρίων κινδύνου θα πρέπει να λαμβάνονται υπόψη οι σχετικές εκτιμήσεις κινδύνου και τα σενάρια κινδύνου σε επίπεδο Ένωσης, συμπεριλαμβανομένης της ανάγκης αποφυγής επικαλύψεων, όπως η εκτίμηση κινδύνου και τα σενάρια κινδύνου που απαιτούνται στα συμπεράσματα του Συμβουλίου σχετικά με τη διαμόρφωση της στάσης της Ευρωπαϊκής Ένωσης στον κυβερνοχώρο που εκπονεί η Επιτροπή, ο ύπατος εκπρόσωπος της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας («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 ***που θεσπίστηκε με τον κανονισμό (ΕΕ) 2018/1971 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου***[18], οι συντονισμένες εκτιμήσεις κινδύνου για την ασφάλεια κρίσιμων εφοδιαστικών αλυσίδων σε ενωσιακό επίπεδο που πρέπει να διενεργούνται δυνάμει του άρθρου 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[19]. 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.

---

*18* ***Κανονισμός (ΕΕ) 2018/1971 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2018, για την ίδρυση του Φορέα Ευρωπαϊκών Ρυθμιστικών Αρχών για τις Ηλεκτρονικές Επικοινωνίες (BEREC) και του Οργανισμού για την υποστήριξη του BEREC (Υπηρεσία του BEREC), την τροποποίηση του κανονισμού (ΕΕ) 2015/2120 και την κατάργηση του κανονισμού (ΕΚ) αριθ. 1211/2009 (ΕΕ L 321 της 17.12.2018, σ. 1).***

**19** 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 (ΕΕ L 333 της 27.12.2022, σ. 1*)*.

(35) Επιπλέον, ο μηχανισμός έκτακτης ανάγκης ***για την κυβερνοασφάλεια*** θα πρέπει να παρέχει στήριξη για άλλες δράσεις ετοιμότητας και στήριξη για την ετοιμότητα σε άλλους τομείς, οι οποίοι δεν καλύπτονται από τις συντονισμένες δοκιμές ετοιμότητας οντοτήτων που δραστηριοποιούνται σε τομείς ***υψηλής κρισιμότητας ή οντοτήτων που δραστηριοποιούνται σε άλλους κρίσιμους τομείς***. Οι δράσεις αυτές μπορούν να περιλαμβάνουν διάφορα είδη εθνικών δραστηριοτήτων ετοιμότητας.

***(36) Όταν τα κράτη μέλη λαμβάνουν επιχορηγήσεις για τη στήριξη δράσεων ετοιμότητας, οι οντότητες σε τομείς υψηλής κρισιμότητας μπορούν να συμμετέχουν στις εν λόγω δράσεις σε εθελοντική βάση. Αποτελεί ορθή πρακτική, μετά τις εν λόγω δράσεις, οι συμμετέχουσες οντότητες να καταρτίζουν σχέδιο αποκατάστασης για την εφαρμογή τυχόν συνακόλουθων συστάσεων για ειδικά μέτρα, ώστε να αποκομίζονται τα μέγιστα δυνατά οφέλη από τη δράση ετοιμότητας. Μολονότι είναι σημαντικό τα κράτη μέλη να ζητούν, στο πλαίσιο των δράσεων, από τις συμμετέχουσες οντότητες να καταρτίζουν και να εφαρμόζουν τέτοια σχέδια αποκατάστασης, τα κράτη μέλη δεν υποχρεούνται από τον παρόντα κανονισμό να εκτελούν τα αιτήματα αυτά, ούτε και εξουσιοδοτούνται να επιβάλλουν την εκτέλεσή τους. Τα εν λόγω αιτήματα δεν θίγουν τις απαιτήσεις που ισχύουν για τις οντότητες ούτε και τις εποπτικές εξουσίες των αρμόδιων αρχών, σύμφωνα με την οδηγία (ΕΕ) 2022/2555.***

(37) Ο μηχανισμός έκτακτης ανάγκης ***για την κυβερνοασφάλεια*** θα πρέπει να παρέχει επίσης βοήθεια για δράσεις αντιμετώπισης περιστατικών με σκοπό τον μετριασμό των επιπτώσεων σημαντικών περιστατικών κυβερνοασφάλειας και περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας, τη στήριξη της ***αρχικής*** ανάκαμψης 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 στους πολίτες.

(38) Ο μηχανισμός έκτακτης ανάγκης ***για την κυβερνοασφάλεια*** θα πρέπει να στηρίζει ***την τεχνική*** συνδρομή που παρέχεται από ***ένα κράτος μέλος σε άλλο*** κράτος μέλος που επηρεάζεται από σημαντικό περιστατικό κυβερνοασφάλειας ή περιστατικό κυβερνοασφάλειας μεγάλης κλίμακας, μεταξύ άλλων από ***τις*** CSIRT που ***αναφέρονται*** στο άρθρο ***11 παράγραφος 3 στοιχείο στ)*** της οδηγίας (ΕΕ) 2022/2555. Τα κράτη μέλη που παρέχουν ***τέτοια*** 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.

***(39) Δεδομένου του ουσιώδους ρόλου που διαδραματίζουν οι ιδιωτικές επιχειρήσεις στον εντοπισμό περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας και περιστατικών ισοδύναμων με περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας, στην ετοιμότητα για τέτοια περιστατικά και στην αντιμετώπισή τους, είναι σημαντικό να αναγνωριστεί η αξία της εθελοντικής και αφιλοκερδούς συνεργασίας με τις εν λόγω επιχειρήσεις, στο πλαίσιο της οποίας αυτές προσφέρουν υπηρεσίες χωρίς αμοιβή σε περιπτώσεις περιστατικών και κρίσεων κυβερνοασφάλειας μεγάλης κλίμακας, και περιστατικών και κρίσεων ισοδύναμων με περιστατικά και κρίσεις κυβερνοασφάλειας μεγάλης κλίμακας. Ο ENISA, σε συνεργασία με το EU-CyCLONe, θα μπορούσε να παρακολουθεί την εξέλιξη των εν λόγω αφιλοκερδών πρωτοβουλιών και να προωθεί τη συμμόρφωσή τους με τα κριτήρια που ισχύουν για τους αξιόπιστους παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας βάσει του παρόντος κανονισμού, μεταξύ άλλων σε σχέση με την αξιοπιστία των ιδιωτικών επιχειρήσεων, την εμπειρία τους, καθώς και την ικανότητά τους να χειρίζονται ευαίσθητες πληροφορίες με ασφαλή τρόπο.***

***(40)*** ***Στο πλαίσιο του μηχανισμού έκτακτης ανάγκης για την κυβερνοασφάλεια,*** θα πρέπει σταδιακά να δημιουργηθεί εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, η οποία θα αποτελείται από υπηρεσίες από ***αξιόπιστους*** παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας ▌για την υποστήριξη δράσεων αντιμετώπισης και ***αρχικής*** ανάκαμψης σε περιπτώσεις σημαντικών ***περιστατικών κυβερνοασφάλειας, περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας ή περιστατικών ισοδύναμων με περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας που επηρεάζουν κράτη μέλη, θεσμικά και λοιπά όργανα ή οργανισμούς της Ένωσης, ή τρίτες χώρες συνδεδεμένες με το*** πρόγραμμα «Ψηφιακή Ευρώπη»***.*** Η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας θα πρέπει να διασφαλίζει τη διαθεσιμότητα και την ετοιμότητα των υπηρεσιών. ***Θα πρέπει επομένως να περιλαμβάνει υπηρεσίες που έχουν δεσμευτεί εκ των προτέρων, συμπεριλαμβανομένων, για παράδειγμα, ικανοτήτων που βρίσκονται σε ετοιμότητα και μπορούν να αναπτυχθούν σε σύντομο χρονικό διάστημα.*** Οι υπηρεσίες από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας θα πρέπει να χρησιμοποιούνται για τη στήριξη των εθνικών αρχών όσον αφορά την παροχή βοήθειας σε επηρεαζόμενες οντότητες που δραστηριοποιούνται σε ***τομείς υψηλής κρισιμότητας ή σε επηρεαζόμενες οντότητες που δραστηριοποιούνται σε άλλους κρίσιμους τομείς***, συμπληρωματικά προς τις δικές τους δράσεις σε εθνικό επίπεδο. ***Οι υπηρεσίες από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας θα πρέπει να μπορούν επίσης να χρησιμεύσουν για τη στήριξη των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης, υπό παρόμοιες συνθήκες. Η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας θα μπορούσε επίσης να συμβάλει στην ενίσχυση της ανταγωνιστικής θέσης της βιομηχανίας και των υπηρεσιών στην Ένωση, σε ολόκληρη την ψηφιακή οικονομία, συμπεριλαμβανομένων των πολύ μικρών και των μικρών και μεσαίων επιχειρήσεων, καθώς και των νεοφυών επιχειρήσεων, μεταξύ άλλων με την παροχή κινήτρων για επενδύσεις στην έρευνα και την καινοτομία. Είναι σημαντικό να λαμβάνεται υπόψη το ευρωπαϊκό πλαίσιο δεξιοτήτων κυβερνοασφάλειας του ENISA κατά την προμήθεια υπηρεσιών για την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας.*** Όταν ζητούν στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, ***οι χρήστες θα πρέπει να περιλαμβάνουν στην αίτησή τους κατάλληλες πληροφορίες σχετικά με την επηρεαζόμενη οντότητα και τις δυνητικές επιπτώσεις, πληροφορίες σχετικά με την υπηρεσία που ζητείται από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, και πληροφορίες σχετικά με τη στήριξη που παρέχεται στην επηρεαζόμενη οντότητα σε εθνικό επίπεδο, οι οποίες θα πρέπει να***

***λαμβάνονται υπόψη κατά την αξιολόγηση του αιτήματος του αιτούντος. Για να διασφαλίζεται η συμπληρωματικότητα με άλλες μορφές στήριξης που έχει στη διάθεσή της η επηρεαζόμενη οντότητα, το αίτημα θα πρέπει επίσης να περιλαμβάνει, κατά περίπτωση, πληροφορίες σχετικά με τις συμβατικές ρυθμίσεις που ισχύουν για τις υπηρεσίες αντιμετώπισης περιστατικών και αρχικής ανάκαμψης, καθώς και σχετικά με τα ασφαλιστήρια συμβόλαια που ενδέχεται να καλύπτουν τέτοιου είδους περιστατικά.***

***(41) Προκειμένου να διασφαλιστεί η αποτελεσματική χρήση της ενωσιακής χρηματοδότησης, οι προδεσμευμένες υπηρεσίες στο πλαίσιο της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας θα πρέπει να μετατραπούν, σύμφωνα με τη σχετική σύμβαση, σε υπηρεσίες ετοιμότητας που σχετίζονται με την πρόληψη και την αντιμετώπιση περιστατικών, σε περίπτωση που οι εν λόγω προδεσμευμένες υπηρεσίες δεν χρησιμοποιούνται για την αντιμετώπιση περιστατικών κατά τη διάρκεια της περιόδου για την οποία έχουν προδεσμευτεί. Οι υπηρεσίες αυτές θα πρέπει να είναι συμπληρωματικές και θα πρέπει να μην αλληλεπικαλύπτονται με τις δράσεις ετοιμότητας που θα διαχειρίζεται το ΕΚΑΚ.***

***(42) Τα αιτήματα για στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας τα οποία υποβάλλονται από τις αρχές διαχείρισης κρίσεων στον κυβερνοχώρο και τις CSIRT των κρατών μελών, ή τη CERT-ΕΕ, εξ ονόματος των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης, θα πρέπει να αξιολογούνται από την αναθέτουσα αρχή. Στην περίπτωση που έχει ανατεθεί στον ENISA η διαχείριση και η λειτουργία της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, η αναθέτουσα αρχή είναι ο ENISA. Τα αιτήματα στήριξης που υποβάλλονται από τρίτες χώρες συνδεδεμένες με το*** πρόγραμμα «Ψηφιακή Ευρώπη» ***θα πρέπει να αξιολογούνται από την Επιτροπή. Για να διευκολυνθεί η υποβολή και η αξιολόγηση των αιτημάτων στήριξης, ο ENISA θα μπορούσε να δημιουργήσει μια ασφαλή πλατφόρμα.***

***(43) Όταν λαμβάνονται πολλαπλά παράλληλα αιτήματα, τα εν λόγω αιτήματα θα πρέπει να ιεραρχούνται σύμφωνα με τα κριτήρια που ορίζονται στον παρόντα κανονισμό. Υπό το πρίσμα των γενικών στόχων του παρόντος κανονισμού, τα κριτήρια αυτά θα πρέπει να περιλαμβάνουν την κλίμακα και τη σοβαρότητα του περιστατικού, το είδος της επηρεαζόμενης οντότητας, τις δυνητικές επιπτώσεις του περιστατικού στα επηρεαζόμενα κράτη μέλη και τους επηρεαζόμενους χρήστες, τον δυνητικό διασυνοριακό χαρακτήρα του περιστατικού και τον κίνδυνο δευτερογενών επιπτώσεων, καθώς και τα μέτρα που έχει ήδη λάβει ο χρήστης για να βοηθήσει στην αντιμετώπιση και την αρχική ανάκαμψη. Υπό το πρίσμα των εν λόγω στόχων και δεδομένου ότι τα αιτήματα των χρηστών των κρατών μελών αποσκοπούν αποκλειστικά στη στήριξη σε ολόκληρη την Ένωση οντοτήτων που δραστηριοποιούνται σε τομείς υψηλής κρισιμότητας ή οντοτήτων που δραστηριοποιούνται σε άλλους κρίσιμους τομείς, είναι σκόπιμο να δίνεται υψηλότερη προτεραιότητα στα αιτήματα των χρηστών των κρατών μελών όταν δύο ή περισσότερα αιτήματα αξιολογούνται ως ισότιμα βάσει των εν λόγω κριτηρίων. Αυτό ισχύει με την επιφύλαξη τυχόν υποχρεώσεων που ενδέχεται να έχουν τα κράτη μέλη, βάσει των σχετικών συμφωνιών υποδοχής, να λαμβάνουν μέτρα για την προστασία και τη συνδρομή των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης.***

***(44) Η Επιτροπή θα πρέπει να έχει τη συνολική ευθύνη για την εφαρμογή της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. Δεδομένης της εκτεταμένης εμπειρίας που έχει αποκτήσει ο ENISA από τη δράση στήριξης της κυβερνοασφάλειας, ο ENISA είναι ο πλέον κατάλληλος οργανισμός για την υλοποίηση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. Ως εκ τούτου, η Επιτροπή θα πρέπει να αναθέτει στον ENISA, εν μέρει ή, όταν κρίνεται σκόπιμο, εξ ολοκλήρου τη λειτουργία και τη διαχείριση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. Η ανάθεση θα πρέπει να πραγματοποιείται σύμφωνα με τους ισχύοντες κανόνες του κανονισμού (ΕΕ, Ευρατόμ) 2024/2509 και, ειδικότερα, θα πρέπει να εξαρτάται από την εκπλήρωση των σχετικών προϋποθέσεων για την υπογραφή συμφωνίας συνεισφοράς. Τυχόν πτυχές της λειτουργίας και της διαχείρισης της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας που δεν ανατίθενται στον ENISA θα πρέπει να υπόκεινται σε άμεση διαχείριση από την Επιτροπή, μεταξύ άλλων πριν από την υπογραφή της συμφωνίας συνεισφοράς.***

***(45) Τα κράτη μέλη θα πρέπει να διαδραματίζουν καίριο ρόλο στη σύσταση και την ανάπτυξη της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, καθώς και κατά την περίοδο μετά την ανάπτυξή της. Δεδομένου ότι ο κανονισμός (ΕΕ) 2021/694 είναι η σχετική βασική πράξη για δράσεις υλοποίησης της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, οι δράσεις στο πλαίσιο της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας θα πρέπει να προβλέπονται στα προγράμματα εργασίας που αναφέρονται στο άρθρο 24 του κανονισμού (ΕΕ) 2021/694. Δυνάμει της παραγράφου 6 του εν λόγω άρθρου, τα εν λόγω προγράμματα εργασίας πρέπει να εγκρίνονται από την Επιτροπή με εκτελεστικές πράξεις σύμφωνα με τη διαδικασία εξέτασης. Επιπλέον, η Επιτροπή, σε συντονισμό με την ομάδα συνεργασίας NIS, θα πρέπει να καθορίσει τις προτεραιότητες και την εξέλιξη της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας.***

***(46) Οι συμβάσεις που συνάπτονται στο πλαίσιο της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας δεν θα πρέπει να επηρεάζουν τη διεπιχειρησιακή σχέση και τις υφιστάμενες υποχρεώσεις μεταξύ της επηρεαζόμενης οντότητας ή των χρηστών και του παρόχου υπηρεσιών.***

(47) 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 και απαιτήσεων 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 των κρατών μελών, των οντοτήτων που δραστηριοποιούνται σε ***τομείς υψηλής κρισιμότητας ή*** των οντοτήτων που δραστηριοποιούνται σε ***άλλους κρίσιμους τομείς***. ***Προκειμένου να καλύπτονται οι συγκεκριμένες ανάγκες των κρατών μελών, κατά την προμήθεια υπηρεσιών για την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, η αναθέτουσα αρχή θα πρέπει, κατά περίπτωση, να αναπτύσσει κριτήρια επιλογής και απαιτήσεις πέραν εκείνων που ορίζονται στον παρόντα κανονισμό. Είναι σημαντικό να ενθαρρυνθεί η συμμετοχή μικρότερων παρόχων δραστηριοποιούμενων σε περιφερειακό και τοπικό επίπεδο.***

***(48) Κατά την επιλογή παρόχων που θα συμπεριληφθούν στην εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, η αναθέτουσα αρχή θα πρέπει να έχει ως στόχο να διασφαλίζει ότι η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, εξεταζόμενη στο σύνολό της, περιλαμβάνει παρόχους που είναι σε θέση να ανταποκρίνονται στις γλωσσικές απαιτήσεις των χρηστών. Για τον σκοπό αυτό, η αναθέτουσα αρχή, πριν από την κατάρτιση της συγγραφής υποχρεώσεων, θα πρέπει να διερευνά κατά πόσον οι δυνητικοί χρήστες της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας έχουν ειδικές γλωσσικές απαιτήσεις, ώστε οι υπηρεσίες στήριξης της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας να μπορούν να παρέχονται σε μία από τις επίσημες γλώσσες των θεσμικών οργάνων της Ένωσης ή των κρατών μελών που είναι πιθανό να είναι κατανοητή από τον χρήστη ή την επηρεαζόμενη οντότητα. Σε περίπτωση που ένας χρήστης χρειάζεται περισσότερες από μία γλώσσες για την παροχή υπηρεσιών στήριξης της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας και οι υπηρεσίες έχουν αποκτηθεί στις εν λόγω γλώσσες για τον εν λόγω χρήστη, ο χρήστης θα πρέπει να είναι σε θέση να προσδιορίσει, στο αίτημα για στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, σε ποιες από τις γλώσσες αυτές θα πρέπει να παρέχονται οι υπηρεσίες σε σχέση με το συγκεκριμένο περιστατικό που οδήγησε στο αίτημα.***

(49) Για τη στήριξη της δημιουργίας της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, ***είναι σημαντικό*** η Επιτροπή ***να*** ζητήσει από τον ENISA να καταρτίσει υποψήφιο σχήμα πιστοποίησης ***της κυβερνοασφάλειας*** για διαχειριζόμενες υπηρεσίες ασφάλειας σύμφωνα με τον κανονισμό (ΕΕ) 2019/881, στους τομείς που καλύπτονται από τον μηχανισμό έκτακτης ανάγκης ***για την κυβερνοασφάλεια***.

(50) 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 περιστατικών κυβερνοασφάλειας και περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας, ***η Επιτροπή ή*** το EU-CyCLONe θα πρέπει να είναι σε θέση να ζητούν από τον ENISA, με τη στήριξη του δικτύου CSIRT και με την έγκριση των οικείων κρατών μελών***,*** να εξετάζει και να αξιολογεί κυβερνοαπειλές, ***γνωστές εκμεταλλεύσιμες*** ευπάθειες και δράσεις μετριασμού σε σχέση με συγκεκριμένο σημαντικό περιστατικό κυβερνοασφάλειας ή περιστατικό κυβερνοασφάλειας μεγάλης κλίμακας. Μετά την ολοκλήρωση της εξέτασης και της αξιολόγησης ενός περιστατικού, ο ENISA θα πρέπει να συντάσσει έκθεση εξέτασης περιστατικού, σε συνεργασία με ***το οικείο κράτος μέλος,*** τα σχετικά ενδιαφερόμενα μέρη, συμπεριλαμβανομένων εκπροσώπων του ιδιωτικού τομέα, ▌της Επιτροπής και άλλων σχετικών θεσμικών και λοιπών οργάνων***, υπηρεσιών*** και οργανισμών της Ένωσης. 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 ***στο EU-CyCLONe, στο δίκτυο CSIRT και στην Επιτροπή και θα πρέπει*** να αξιοποιείται στο πλαίσιο των εργασιών ***τους καθώς και των εργασιών του ENISA***. Όταν το περιστατικό αφορά τρίτη χώρα ***συνδεδεμένη με το*** πρόγραμμα «Ψηφιακή Ευρώπη», η Επιτροπή θα πρέπει επίσης να κοινοποιεί την έκθεση στον ύπατο εκπρόσωπο.

(51) 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 περιστατικά κυβερνοασφάλειας και περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας συμβάλλει συνολικά στην προστασία της Ένωσης***, και ιδίως στην προστασία της εσωτερικής της αγοράς και της βιομηχανίας της***. ***Οι δραστηριότητες αυτές θα μπορούσαν να συμβάλουν περαιτέρω στη διπλωματία της Ένωσης στον κυβερνοχώρο. Κατά συνέπεια, οι τρίτες χώρες συνδεδεμένες με το*** πρόγραμμα «Ψηφιακή Ευρώπη» θα πρέπει να έχουν τη δυνατότητα να ζητούν στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, ***στο σύνολο ή σε μέρος της επικράτειάς τους, όταν αυτό προβλέπεται στη συμφωνία μέσω της οποίας η τρίτη χώρα συνδέεται*** με το πρόγραμμα «Ψηφιακή Ευρώπη». Η χρηματοδότηση τρίτων χωρών συνδεδεμένων ***με το*** πρόγραμμα «Ψηφιακή Ευρώπη» 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 ***αρχικής*** ανάκαμψης από σημαντικά περιστατικά κυβερνοασφάλειας ή περιστατικά ισοδύναμα με περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας.

***(52)*** ***Οι προϋποθέσεις που καθορίζονται στον παρόντα κανονισμό για την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας και για τους αξιόπιστους παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας θα πρέπει να εφαρμόζονται κατά την παροχή στήριξης στις τρίτες χώρες συνδεδεμένες με το*** πρόγραμμα «Ψηφιακή Ευρώπη»***. Οι τρίτες χώρες συνδεδεμένες με το*** πρόγραμμα «Ψηφιακή Ευρώπη» ***θα πρέπει να είναι σε θέση να ζητούν στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας όταν οι στοχευόμενες οντότητες για τις οποίες ζητούν στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας είναι οντότητες που δραστηριοποιούνται σε τομείς υψηλής κρισιμότητας ή οντότητες που δραστηριοποιούνται σε άλλους κρίσιμους τομείς και όταν τα περιστατικά που εντοπίζονται οδηγούν σε σημαντικές λειτουργικές διαταραχές ή ενδέχεται να έχουν δευτερογενείς επιπτώσεις στην Ένωση. Οι τρίτες χώρες συνδεδεμένες με το*** πρόγραμμα «Ψηφιακή Ευρώπη» ***θα πρέπει να είναι επιλέξιμες για στήριξη μόνο όταν η συμφωνία μέσω της οποίας συνδέονται με το πρόγραμμα «Ψηφιακή Ευρώπη» προβλέπει ρητά την εν λόγω στήριξη. Επιπλέον, οι εν λόγω τρίτες χώρες θα πρέπει να παραμένουν επιλέξιμες μόνο εφόσον πληρούνται τρία κριτήρια. Πρώτον, η τρίτη χώρα θα πρέπει να συμμορφώνεται πλήρως με τους σχετικούς όρους της εν λόγω συμφωνίας. Δεύτερον, δεδομένου του συμπληρωματικού χαρακτήρα της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, η τρίτη χώρα θα πρέπει να έχει λάβει κατάλληλα μέτρα για την προετοιμασία για σημαντικά περιστατικά κυβερνοασφάλειας ή για περιστατικά ισοδύναμα με περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας. Τρίτον, η παροχή στήριξης από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας θα πρέπει να συνάδει με την πολιτική της Ένωσης και τις συνολικές σχέσεις της με την εν λόγω χώρα, καθώς και με άλλες πολιτικές της Ένωσης στον τομέα της ασφάλειας. Στο πλαίσιο της αξιολόγησής της σχετικά με τη συμμόρφωση με το τρίτο αυτό κριτήριο, η Επιτροπή θα πρέπει να διαβουλεύεται με τον ύπατο εκπρόσωπο ώστε η χορήγηση της εν λόγω στήριξης να ευθυγραμμίζεται με την κοινή εξωτερική πολιτική και πολιτική ασφαλείας.***

***(53)*** ***Η παροχή στήριξης σε τρίτες χώρες συνδεδεμένες με το*** πρόγραμμα «Ψηφιακή Ευρώπη» ***μπορεί να επηρεάσει τις σχέσεις με τρίτες χώρες και την πολιτική ασφάλειας της Ένωσης, μεταξύ άλλων στο πλαίσιο της κοινής εξωτερικής πολιτικής και πολιτικής ασφαλείας καθώς και της κοινής πολιτικής ασφάλειας και άμυνας. Κατά συνέπεια, είναι σκόπιμο να ανατεθούν στο Συμβούλιο εκτελεστικές αρμοδιότητες ώστε να εγκρίνει και να προσδιορίζει το χρονικό διάστημα κατά το οποίο μπορεί να παρέχεται η εν λόγω στήριξη. Το Συμβούλιο θα πρέπει να ενεργεί βάσει πρότασης της Επιτροπής, λαμβάνοντας δεόντως υπόψη την αξιολόγηση της Επιτροπής ως προς τα εν λόγω τρία κριτήρια. Το ίδιο θα πρέπει να ισχύει και για τις ανανεώσεις και τις προτάσεις τροποποίησης ή ανάκλησης τέτοιων πράξεων. Όταν, σε εξαιρετικές περιστάσεις, το Συμβούλιο κρίνει ότι υπήρξε σημαντική μεταβολή των συνθηκών σε σχέση με το τρίτο κριτήριο, το Συμβούλιο θα πρέπει να είναι σε θέση να αποφασίζει με δική του πρωτοβουλία για την τροποποίηση ή ανάκληση μιας εκτελεστικής πράξης, χωρίς να αναμένει πρόταση της Επιτροπής. Τέτοιες σημαντικές μεταβολές είναι πιθανό να καθιστούν αναγκαία την ανάληψη επείγουσας δράσης, να έχουν ιδιαίτερα σημαντικές επιπτώσεις στις σχέσεις με τρίτες χώρες και να μην απαιτούν λεπτομερή αξιολόγηση εκ των προτέρων από την Επιτροπή. Επιπλέον, η Επιτροπή θα πρέπει να συνεργάζεται με τον ύπατο εκπρόσωπο όσον αφορά τα εν λόγω αιτήματα για τη στήριξη από τρίτες χώρες συνδεδεμένες με το*** πρόγραμμα «Ψηφιακή Ευρώπη» ***και την υλοποίηση της στήριξης που έχει χορηγηθεί σε αυτές τις τρίτες χώρες. Η Επιτροπή θα πρέπει επίσης να λαμβάνει υπόψη τυχόν απόψεις που παρέχει ο ENISA σχετικά με αυτά τα αιτήματα και τη στήριξη. Η Επιτροπή θα πρέπει να ενημερώνει το Συμβούλιο όσον αφορά το αποτέλεσμα της αξιολόγησης των αιτημάτων, συμπεριλαμβανομένων των σχετικών εκτιμήσεων που διατυπώνονται στο πλαίσιο αυτό, καθώς και όσον αφορά τις υπηρεσίες που αναπτύσσονται.***

***(54) Στην ανακοίνωση της Επιτροπής, της 18ης Απριλίου 2023, σχετικά με την Ακαδημία Κυβερνοδεξιοτήτων, αναγνωρίζεται η έλλειψη ειδικευμένων επαγγελματιών. Οι δεξιότητες αυτές είναι απαραίτητες για την επίτευξη των στόχων του παρόντος κανονισμού. Η Ένωση χρειάζεται επειγόντως επαγγελματίες με τις κατάλληλες δεξιότητες και ικανότητες για την πρόληψη, τον εντοπισμό και την αποτροπή κυβερνοεπιθέσεων, καθώς και για την προστασία της Ένωσης, συμπεριλαμβανομένων των πλέον κρίσιμων υποδομών της, από τέτοιες επιθέσεις και για τη διασφάλιση της ανθεκτικότητάς της. Για τον σκοπό αυτό, είναι σημαντικό να ενθαρρυνθεί η συνεργασία μεταξύ των ενδιαφερόμενων μερών, συμπεριλαμβανομένων του ιδιωτικού τομέα, της ακαδημαϊκής κοινότητας και του δημόσιου τομέα. Είναι εξίσου σημαντικό να δημιουργηθούν συνέργειες, στο σύνολο των εδαφών της Ένωσης, όσον αφορά τις επενδύσεις στην εκπαίδευση και την κατάρτιση, ώστε να υπάρξουν διασφαλίσεις για την αποφυγή της διαρροής εγκεφάλων ή της διεύρυνσης του χάσματος δεξιοτήτων μεταξύ των περιφερειών. Είναι επείγον να γεφυρωθεί το χάσμα δεξιοτήτων κυβερνοασφάλειας, με ιδιαίτερη έμφαση στη μείωση του έμφυλου χάσματος στο εργατικό δυναμικό στον τομέα της κυβερνοασφάλειας, ώστε να προωθηθεί η παρουσία και η συμμετοχή γυναικών στον σχεδιασμό της ψηφιακής διακυβέρνησης.***

***(55)*** ***Προκειμένου να τονωθεί η καινοτομία στην ψηφιακή ενιαία αγορά, είναι σημαντικό να ενισχυθεί η έρευνα και η καινοτομία στον τομέα της κυβερνοασφάλειας, με σκοπό την συμβολή στην αύξηση της ανθεκτικότητας των κρατών μελών και της ανοικτής στρατηγικής αυτονομίας της Ένωσης, που αποτελούν στόχους του παρόντος κανονισμού. Οι συνέργειες είναι απαραίτητες για την ενίσχυση της συνεργασίας και του συντονισμού μεταξύ των διαφόρων ενδιαφερόμενων μερών, συμπεριλαμβανομένων του ιδιωτικού τομέα, της κοινωνίας των πολιτών και της ακαδημαϊκής κοινότητας.***

***(56)*** ***Ο παρών κανονισμός θα πρέπει να λαμβάνει υπόψη τη δέσμευση στην κοινή δήλωση της 26ης Ιανουαρίου 2022 του Ευρωπαϊκού Κοινοβουλίου, του Συμβουλίου και της Επιτροπής, με τίτλο «Ευρωπαϊκή διακήρυξη σχετικά με τα ψηφιακά δικαιώματα και τις ψηφιακές αρχές για την ψηφιακή δεκαετία», όσον αφορά την προστασία των συμφερόντων των δημοκρατιών, των πολιτών, των επιχειρήσεων και των δημόσιων οργανισμών της Ένωσης από τους κινδύνους κυβερνοασφάλειας και το κυβερνοέγκλημα, συμπεριλαμβανομένων των παραβιάσεων δεδομένων και της κλοπής ή χειραγώγησης ταυτότητας.***

***(57)*** ***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 προσδιοριστούν οι τύποι και ο αριθμός των υπηρεσιών αντιμετώπισης που απαιτούνται για την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας. Είναι ιδιαίτερα σημαντικό η Επιτροπή να διεξάγει, κατά τις προπαρασκευαστικές της εργασίες, τις κατάλληλες διαβουλεύσεις, μεταξύ άλλων σε επίπεδο εμπειρογνωμόνων, οι οποίες να πραγματοποιούνται σύμφωνα με τις αρχές που ορίζονται στη διοργανική συμφωνία της 13ης Απριλίου 2016 για τη βελτίωση του νομοθετικού έργου[20]. 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 εμπειρογνώμονες των κρατών μελών, και οι εμπειρογνώμονές τους να έχουν συστηματικά πρόσβαση στις συνεδριάσεις των ομάδων εμπειρογνωμόνων της Επιτροπής που ασχολούνται με την προετοιμασία κατ' εξουσιοδότηση πράξεων.***

(58) Προκειμένου να διασφαλιστούν ενιαίες προϋποθέσεις για την εφαρμογή του παρόντος κανονισμού, θα πρέπει να ανατεθούν στην Επιτροπή εκτελεστικές αρμοδιότητες ***για τον περαιτέρω προσδιορισμό των λεπτομερών ρυθμίσεων για την κατανομή των υπηρεσιών στήριξης 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[21].***

---

*20* *ΕΕ L 123 της 12.5.2016, σ. 1.* ***ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.***

**21** ***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: http://data.europa.eu/eli/reg/2011/182/oj).***

***(59)*** ***Με την επιφύλαξη των κανόνων που αφορούν τον ετήσιο προϋπολογισμό της Ένωσης δυνάμει των Συνθηκών, η Επιτροπή θα πρέπει να λαμβάνει υπόψη τις υποχρεώσεις που απορρέουν από τον παρόντα κανονισμό κατά την αξιολόγηση των αναγκών προϋπολογισμού και στελέχωσης του ENISA.***

***(60)*** ***Η Επιτροπή θα πρέπει να διενεργεί σε τακτική βάση αξιολόγηση των μέτρων που προβλέπονται στον παρόντα κανονισμό. Η πρώτη τέτοια αξιολόγηση θα πρέπει να πραγματοποιηθεί κατά τα πρώτα δύο έτη από την ημερομηνία εφαρμογής του παρόντος κανονισμού και οι επόμενες αξιολογήσεις τουλάχιστον ανά τετραετία, λαμβανομένου υπόψη του χρονοδιαγράμματος της αναθεώρησης του πολυετούς δημοσιονομικού πλαισίου που θεσπίστηκε δυνάμει του άρθρου 312 ΣΛΕΕ. Η Επιτροπή θα πρέπει να υποβάλει στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο έκθεση σχετικά με την πρόοδο που σημειώνεται. Για την αξιολόγηση των διαφόρων στοιχείων που απαιτούνται, συμπεριλαμβανομένου του εύρους των πληροφοριών που ανταλλάσσονται στο πλαίσιο του ευρωπαϊκού συστήματος προειδοποίησης για την κυβερνοασφάλεια, η Επιτροπή θα πρέπει να βασίζεται αποκλειστικά σε πληροφορίες που είναι άμεσα διαθέσιμες ή παρέχονται οικειοθελώς. Λαμβανομένων υπόψη των γεωπολιτικών εξελίξεων και προκειμένου να διασφαλιστούν η συνέχεια και η περαιτέρω ανάπτυξη των μέτρων που ορίζονται στον παρόντα κανονισμό μετά το 2027, είναι σημαντικό να αξιολογήσει η Επιτροπή την αναγκαιότητα διάθεσης κατάλληλου προϋπολογισμού στο πολυετές δημοσιονομικό πλαίσιο για την περίοδο 2028 έως 2034.***

(61) ***Δεδομένου ότι οι στόχοι του παρόντος κανονισμού, ήτοι να ενισχυθεί η ανταγωνιστική θέση της βιομηχανίας και των υπηρεσιών στην Ένωση σε ολόκληρη την ψηφιακή οικονομία, και να συμβάλλει στην τεχνολογική κυριαρχία και την ανοικτή στρατηγική αυτονομία της Ένωσης στον τομέα της κυβερνοασφάλειας, δεν μπορούν να επιτευχθούν ικανοποιητικά από τα κράτη μέλη, μπορούν όμως, λόγω της κλίμακας ή των αποτελεσμάτων της δράσης, να επιτευχθούν καλύτερα σε επίπεδο Ένωσης, η Ένωση δύναται να λάβει μέτρα σύμφωνα με την αρχή της επικουρικότητας του άρθρου 5 ΣΕΕ. Σύμφωνα με την αρχή της αναλογικότητας όπως διατυπώνεται στο εν λόγω άρθρο, ο παρών κανονισμός δεν υπερβαίνει τα αναγκαία όρια για την επίτευξη των στόχων αυτών,***

ΕΞΕΔΩΣΑΝ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

Κεφάλαιο I

ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

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 κυβερνοαπειλές και περιστατικά κυβερνοασφάλειας, ιδίως θεσπίζοντας:

α) ***πανευρωπαϊκό δίκτυο κυβερνοκόμβων (ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια)*** για την οικοδόμηση και ενίσχυση ***συντονισμένων*** ικανοτήτων ανίχνευσης και ***κοινών ικανοτήτων*** αντίληψης της κατάστασης·

β) μηχανισμό έκτακτης ανάγκης για την κυβερνοασφάλεια με σκοπό τη στήριξη των κρατών μελών όσον αφορά την προετοιμασία, την αντιμετώπιση***, τον μετριασμό των επιπτώσεων και την αρχική*** ανάκαμψη από σημαντικά ***περιστατικά κυβερνοασφάλειας και περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας και τη στήριξη άλλων χρηστών όσον αφορά την αντιμετώπιση*** σημαντικών ***περιστατικών κυβερνοασφάλειας και περιστατικών ισοδύναμων με περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας·***

γ) ευρωπαϊκό μηχανισμό εξέτασης περιστατικών κυβερνοασφάλειας για την εξέταση και την αξιολόγηση σημαντικών περιστατικών κυβερνοασφάλειας ή περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας.

2. ***Ο παρών κανονισμός έχει ως στόχο να επιτευχθούν οι γενικοί στόχοι της ενίσχυσης της ανταγωνιστικής θέσης της βιομηχανίας και των υπηρεσιών στην Ένωση σε ολόκληρη την ψηφιακή οικονομία, συμπεριλαμβανομένων των πολύ μικρών και των μικρών και μεσαίων επιχειρήσεων, καθώς και των νεοφυών επιχειρήσεων, και της συμβολής στην τεχνολογική κυριαρχία και την ανοικτή στρατηγική αυτονομία της Ένωσης στον τομέα της κυβερνοασφάλειας, μεταξύ άλλων με την τόνωση της καινοτομίας στην ψηφιακή ενιαία αγορά. Οι στόχοι αυτοί επιδιώκονται μέσω της ενίσχυσης της αλληλεγγύης σε επίπεδο Ένωσης, του οικοσυστήματος κυβερνοασφάλειας, και της κυβερνοανθεκτικότητας των κρατών μελών, και μέσω της ανάπτυξης των δεξιοτήτων, της τεχνογνωσίας, των ικανοτήτων και των προσόντων του εργατικού δυναμικού σε σχέση με την κυβερνοασφάλεια.***

*3.* ***Η επίτευξη των γενικών στόχων που αναφέρονται στην παράγραφο 2 επιδιώκεται μέσω των ακόλουθων ειδικών στόχων:***

α) ***ενίσχυση των κοινών και συντονισμένων ενωσιακών ικανοτήτων ανίχνευσης και της κοινής*** αντίληψης της κατάστασης όσον αφορά τις κυβερνοαπειλές και τα περιστατικά ▌·

β) ***αύξηση του βαθμού ετοιμότητας των οντοτήτων που δραστηριοποιούνται σε τομείς υψηλής κρισιμότητας ή των οντοτήτων που δραστηριοποιούνται σε άλλους κρίσιμους τομείς σε ολόκληρη την Ένωση, και ενίσχυση της αλληλεγγύης με την ανάπτυξη συντονισμένων ικανοτήτων δοκιμής της ετοιμότητας και ενισχυμένων ικανοτήτων αντιμετώπισης και ανάκαμψης για την διαχείριση σημαντικών περιστατικών κυβερνοασφάλειας, περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας, και περιστατικών ισοδύναμων με περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας, συμπεριλαμβανομένης της δυνατότητας να διατίθεται σε τρίτες χώρες συνδεδεμένες με το*** πρόγραμμα «Ψηφιακή Ευρώπη» ***ενωσιακή στήριξη για την αντιμετώπιση περιστατικών κυβερνοασφάλειας·***

γ) ενίσχυση της ανθεκτικότητας της Ένωσης και συμβολή στην αποτελεσματική αντιμετώπιση περιστατικών με την εξέταση και την αξιολόγηση σημαντικών περιστατικών κυβερνοασφάλειας ή περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας, μεταξύ άλλων με την άντληση διδαγμάτων και, κατά περίπτωση, συστάσεις. ▌

▌

***4.*** ***Οι δράσεις στο πλαίσιο του παρόντος κανονισμού διεξάγονται με τον δέοντα σεβασμό προς τις αρμοδιότητες των κρατών μελών και είναι συμπληρωματικές προς τις δραστηριότητες που διεξάγονται από το δίκτυο CSIRT, το EU-CyCLONe και την ομάδα συνεργασίας NIS.***

5. Ο παρών κανονισμός δεν θίγει ***τις ουσιώδεις κρατικές λειτουργίες των κρατών μελών, ιδίως δε τις λειτουργίες που αποβλέπουν στη διασφάλιση της εδαφικής ακεραιότητας, τη διατήρηση της δημόσιας τάξης και την προστασία της εθνικής ασφάλειας. Ειδικότερα, η εθνική ασφάλεια παραμένει αποκλειστική αρμοδιότητα κάθε κράτους μέλους.***

***6.*** ***Ο διαμοιρασμός ή ανταλλαγή πληροφοριών βάσει του παρόντος κανονισμού που θεωρούνται εμπιστευτικές δυνάμει ενωσιακών ή εθνικών κανόνων περιορίζεται σε ό,τι είναι συναφές και αναλογικό προς τον σκοπό του εν λόγω διαμοιρασμού ή ανταλλαγής. Ο εν λόγω διαμοιρασμός ή ανταλλαγή πληροφοριών στο πλαίσιο του παρόντος κανονισμού διαφυλάσσει το απόρρητο αυτών των πληροφοριών και προστατεύει τα συμφέροντα ασφάλειας και τα εμπορικά συμφέροντα των οικείων οντοτήτων. Δεν συνεπάγεται την παροχή πληροφοριών των οποίων η γνωστοποίηση θα ήταν αντίθετη προς τα ουσιώδη συμφέροντα εθνικής ασφάλειας, δημόσιας ασφάλειας ή άμυνας των κρατών μελών.***

Άρθρο 2

Ορισμοί

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

▌

1) ***«διασυνοριακός κυβερνοκόμβος»: πολυεθνική πλατφόρμα, συσταθείσα με γραπτή συμφωνία κοινοπραξίας, η οποία συγκεντρώνει σε συντονισμένη δομή δικτύου εθνικούς κυβερνοκόμβους από τουλάχιστον τρία κράτη μέλη, και η οποία έχει σχεδιαστεί για την ενίσχυση της παρακολούθησης, της ανίχνευσης και της ανάλυσης κυβερνοαπειλών με σκοπό την πρόληψη περιστατικών και τη στήριξη της παραγωγής πληροφοριών σχετικά με κυβερνοαπειλές, ιδίως μέσω της ανταλλαγής σχετικών δεδομένων και πληροφοριών, ανωνυμοποιημένων κατά περίπτωση,*** καθώς και μέσω της ανταλλαγής εργαλείων αιχμής και της από κοινού ανάπτυξης ικανοτήτων ανίχνευσης, ανάλυσης και πρόληψης και προστασίας στον κυβερνοχώρο σε ένα αξιόπιστο περιβάλλον·

▌

2) «κοινοπραξία υποδοχής»: κοινοπραξία αποτελούμενη από συμμετέχοντα κράτη ***μέλη, τα οποία έχουν συμφωνήσει να δημιουργήσουν εργαλεία, υποδομές και υπηρεσίες για διασυνοριακό κυβερνοκόμβο, να συμβάλουν στην αγορά τέτοιων εργαλείων, υποδομών και υπηρεσιών, καθώς και να συμβάλουν στη λειτουργία του εν λόγω κυβερνοκόμβου·***

***3) «CSIRT»: CSIRT που έχει οριστεί ή συσταθεί σύμφωνα με το άρθρο 10 της οδηγίας (ΕΕ) 2022/2555·***

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

5) «οντότητες που δραστηριοποιούνται σε ***τομείς υψηλής κρισιμότητας***»: τύποι οντοτήτων που απαριθμούνται στο παράρτημα Ι της οδηγίας (ΕΕ) 2022/2555·

6) «οντότητες που δραστηριοποιούνται σε ***άλλους κρίσιμους τομείς***»: τύποι οντοτήτων που απαριθμούνται στα παράρτημα ΙΙ της οδηγίας (ΕΕ) 2022/2555·

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

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

▌

***9)*** ***«περιστατικό»: περιστατικό όπως ορίζεται στο άρθρο 6 σημείο 6) της οδηγίας (ΕΕ) 2022/2555·***

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

***11)*** ***«σοβαρό περιστατικό»: σοβαρό περιστατικό όπως ορίζεται στο άρθρο 3 σημείο 8) του κανονισμού (ΕΕ, Ευρατόμ) 2023/2841 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου***[22]***·***

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

***13)*** ***«περιστατικό ισοδύναμο με περιστατικό κυβερνοασφάλειας μεγάλης κλίμακας»: στην περίπτωση των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης, σοβαρό περιστατικό και, στην περίπτωση τρίτων χωρών συνδεδεμένων με το*** πρόγραμμα «Ψηφιακή Ευρώπη»***, περιστατικό που προκαλεί διαταραχή η οποία υπερβαίνει την ικανότητα της οικείας τρίτης χώρας συνδεδεμένης με το*** πρόγραμμα «Ψηφιακή Ευρώπη» ***να ανταποκριθεί σε αυτήν·***

***14)*** ***«τρίτη χώρα συνδεδεμένη με το*** πρόγραμμα «Ψηφιακή Ευρώπη»***»: τρίτη χώρα η οποία είναι συμβαλλόμενο μέρος συμφωνίας με την Ένωση που επιτρέπει τη συμμετοχή της στο πρόγραμμα «Ψηφιακή Ευρώπη» σύμφωνα με το άρθρο 10 του κανονισμού (ΕΕ) 2021/694·***

---

[22] ***Κανονισμός (ΕΕ, Ευρατόμ) 2023/2841 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 2023, για τον καθορισμό μέτρων για υψηλό κοινό επίπεδο κυβερνοασφάλειας στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης (ΕΕ L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).***

***15)*** ***«αναθέτουσα αρχή»: η Επιτροπή ή, στον βαθμό που η λειτουργία και η διαχείριση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας έχει ανατεθεί στον ENISA δυνάμει του άρθρου 14 παράγραφος 5, ο ENISA·***

***16)*** ***«πάροχος διαχειριζόμενων υπηρεσιών ασφάλειας»: πάροχος διαχειριζόμενων υπηρεσιών ασφάλειας όπως ορίζεται στο άρθρο 6 σημείο 40) της οδηγίας (ΕΕ) 2022/2555·***

17) ***«αξιόπιστοι πάροχοι διαχειριζόμενων υπηρεσιών ασφάλειας»: πάροχοι διαχειριζόμενων υπηρεσιών ασφάλειας οι οποίοι επιλέγονται ώστε να συμπεριληφθούν στην εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας σύμφωνα με το άρθρο 17.***

Κεφάλαιο II

***ΤΟ ΕΥΡΩΠΑΪΚΟ ΣΥΣΤΗΜΑ ΠΡΟΕΙΔΟΠΟΙΗΣΗΣ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ***

Άρθρο 3

Σύσταση ***του ευρωπαϊκού συστήματος προειδοποίησης για την κυβερνοασφάλεια***

1. ***Δημιουργείται πανευρωπαϊκό δίκτυο υποδομών το οποίο αποτελείται από εθνικούς κυβερνοκόμβους και διασυνοριακούς κυβερνοκόμβους που συμμετέχουν σε εθελοντική βάση, με την ονομασία «ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια», προκειμένου να υποστηριχθεί η ανάπτυξη προηγμένων ικανοτήτων για την Ένωση με σκοπό την ενίσχυση των ικανοτήτων ανίχνευσης, ανάλυσης και επεξεργασίας δεδομένων σε σχέση με κυβερνοαπειλές και την πρόληψη περιστατικών στην Ένωση.***

2. ***Το ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια:***

***α) συμβάλλει στη βελτίωση της προστασίας και της αντιμετώπισης κυβερνοαπειλών μέσω της στήριξης, της ενίσχυσης των ικανοτήτων των σχετικών οντοτήτων και της συνεργασίας με αυτές, ιδίως τις CSIRT, το δίκτυο CSIRT, το EU-CyCLONe και τις αρμόδιες αρχές που έχουν οριστεί ή συσταθεί σύμφωνα με το άρθρο 8 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555·***

β) ***συγκεντρώνει σχετικά δεδομένα και πληροφορίες όσον αφορά κυβερνοαπειλές και περιστατικά από διάφορες πηγές εντός των διασυνοριακών κυβερνοκόμβων και διαμοιράζει αναλυμένες ή συγκεντρωτικές πληροφορίες μέσω διασυνοριακών κυβερνοκόμβων, κατά περίπτωση με το δίκτυο CSIRT·***

γ) ***συλλέγει υψηλής ποιότητας και αξιοποιήσιμα στοιχεία και πληροφορίες για κυβερνοαπειλές, και υποστηρίζει την παραγωγή των εν λόγω στοιχείων και πληροφοριών, μέσω της χρήσης εργαλείων αιχμής και προηγμένων τεχνολογιών, και διαμοιράζει τα εν λόγω στοιχεία και τις πληροφορίες σχετικά με κυβερνοαπειλές·***

δ) ***συμβάλλει στην ενίσχυση της συντονισμένης ανίχνευσης κυβερνοαπειλών και της κοινής αντίληψης της κατάστασης σε ολόκληρη την Ένωση, καθώς και στην έκδοση προειδοποιήσεων, μεταξύ άλλων, κατά περίπτωση, με την παροχή συγκεκριμένων συστάσεων σε οντότητες·***

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

***3. Οι δράσεις για την υλοποίηση του ευρωπαϊκού συστήματος προειδοποίησης για την κυβερνοασφάλεια στηρίζονται με χρηματοδότηση από το πρόγραμμα «Ψηφιακή Ευρώπη» και υλοποιούνται σύμφωνα με τον κανονισμό (ΕΕ) 2021/694, ιδίως τον ειδικό στόχο 3.***

Άρθρο 4

***Εθνικοί κυβερνοκόμβοι***

1. ***Όταν ένα κράτος μέλος αποφασίζει να συμμετάσχει στο ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια, ορίζει ή, κατά περίπτωση, δημιουργεί εθνικό κυβερνοκόμβο για τους σκοπούς του παρόντος κανονισμού.***

*2. Ο εθνικός κυβερνοκόμβος είναι μια ενιαία οντότητα που ενεργεί υπό την εξουσία κράτους μέλους. Μπορεί να είναι CSIRT ή, κατά περίπτωση, εθνική αρχή διαχείρισης κρίσεων στον κυβερνοχώρο ή άλλη αρμόδια αρχή που έχει οριστεί ή συσταθεί δυνάμει του άρθρου 8 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555, ή άλλη οντότητα. Ο εθνικός κυβερνοκόμβος:*

*α) έχει την ικανότητα να λειτουργεί ως σημείο αναφοράς και πύλη προς άλλους δημόσιους και ιδιωτικούς οργανισμούς σε εθνικό επίπεδο για τη συλλογή και ανάλυση πληροφοριών σχετικά με κυβερνοαπειλές και περιστατικά, και να συμβάλλει σε διασυνοριακό κυβερνοκόμβο όπως αναφέρεται στο άρθρο 5· και*

*β) είναι σε θέση να ανιχνεύει, να συγκεντρώνει και να αναλύει δεδομένα και στοιχεία σχετικά με κυβερνοαπειλές και περιστατικά, όπως πληροφορίες σχετικά με κυβερνοαπειλές, χρησιμοποιώντας ιδίως τεχνολογίες αιχμής, με σκοπό την πρόληψη περιστατικών.*

*3. Στο πλαίσιο των λειτουργιών που αναφέρονται στην παράγραφο 2 του παρόντος άρθρου, οι εθνικοί κυβερνοκόμβοι μπορούν να συνεργάζονται με οντότητες του ιδιωτικού τομέα για την ανταλλαγή σχετικών δεδομένων και πληροφοριών με σκοπό την ανίχνευση και την πρόληψη κυβερνοαπειλών και περιστατικών, μεταξύ άλλων με τομεακές και διατομεακές κοινότητες βασικών και σημαντικών οντοτήτων όπως αναφέρεται στο άρθρο 3 της οδηγίας (ΕΕ) 2022/2555. Κατά περίπτωση και σύμφωνα με το ενωσιακό και το εθνικό δίκαιο, οι πληροφορίες που ζητούνται ή λαμβάνονται από τους εθνικούς κυβερνοκόμβους μπορούν να περιλαμβάνουν δεδομένα τηλεμετρίας, αισθητήρων και καταγραφής.*

4. *Ένα κράτος μέλος που επιλέγεται σύμφωνα με το άρθρο 9 παράγραφος 1 δεσμεύεται να υποβάλει αίτηση ώστε ο εθνικός του κυβερνοκόμβος να συμμετάσχει σε διασυνοριακό κυβερνοκόμβο.*

Άρθρο 5

***Διασυνοριακοί κυβερνοκόμβοι***

1. ***Όταν τουλάχιστον τρία κράτη μέλη δεσμεύονται να διασφαλίσουν ότι οι εθνικοί τους κυβερνοκόμβοι συνεργάζονται για τον συντονισμό των οικείων δραστηριοτήτων ανίχνευσης και παρακολούθησης κυβερνοαπειλών, τα εν λόγω κράτη μέλη μπορούν να συστήσουν κοινοπραξία υποδοχής για τους σκοπούς του παρόντος κανονισμού («κοινοπραξία υποδοχής»).***

***2. Η κοινοπραξία υποδοχής είναι κοινοπραξία αποτελούμενη από τουλάχιστον τρία συμμετέχοντα κράτη μέλη, τα οποία έχουν συμφωνήσει να δημιουργήσουν εργαλεία, υποδομές και υπηρεσίες για διασυνοριακό κυβερνοκόμβο, να συμβάλουν στην αγορά τέτοιων εργαλείων, υποδομών και υπηρεσιών, καθώς και να συμβάλουν στη λειτουργία του εν λόγω κυβερνοκόμβου, σύμφωνα με την παράγραφο 4.***

3. ***Όταν επιλέγεται κοινοπραξία υποδοχής σύμφωνα με το άρθρο 9 παράγραφος 3, τα μέλη της συνάπτουν γραπτή συμφωνία κοινοπραξίας με την οποία:***

***α)*** καθορίζονται οι εσωτερικές ρυθμίσεις όσον αφορά την εφαρμογή της συμφωνίας υποδοχής και χρήσης ***που αναφέρεται στο άρθρο 9 παράγραφος 3·***

***β) συγκροτείται ο διασυνοριακός κυβερνοκόμβος της κοινοπραξίας υποδοχής· και***

***γ) προβλέπονται οι ειδικές ρήτρες που απαιτούνται σύμφωνα με το άρθρο 6 παράγραφοι 1 και 2.***

***4. Ο διασυνοριακός κυβερνοκόμβος είναι πολυεθνική πλατφόρμα που δημιουργείται με γραπτή συμφωνία κοινοπραξίας, όπως αναφέρεται στην παράγραφο 3. Συγκεντρώνει σε συντονισμένη δομή δικτύου τους εθνικούς κυβερνοκόμβους των κρατών μελών της κοινοπραξίας υποδοχής. Έχει σχεδιαστεί για την ενίσχυση της παρακολούθησης, της ανίχνευσης και της ανάλυσης κυβερνοαπειλών με σκοπό την πρόληψη περιστατικών και τη στήριξη της παραγωγής πληροφοριών σχετικά με κυβερνοαπειλές, ιδίως μέσω της ανταλλαγής σχετικών δεδομένων και πληροφοριών, ανωνυμοποιημένων κατά περίπτωση, καθώς και μέσω της ανταλλαγής εργαλείων αιχμής και της από κοινού ανάπτυξης ικανοτήτων ανίχνευσης, ανάλυσης και πρόληψης και προστασίας στον κυβερνοχώρο σε ένα αξιόπιστο περιβάλλον.***

5. ***Ένας διασυνοριακός κυβερνοκόμβος εκπροσωπείται για νομικούς σκοπούς από ένα μέλος της αντίστοιχης κοινοπραξίας υποδοχής το οποίο ενεργεί ως συντονιστής, ή από την κοινοπραξία υποδοχής, εάν αυτή αποτελεί νομικό πρόσωπο. Η ευθύνη για τη συμμόρφωση του διασυνοριακού κυβερνοκόμβου με τον παρόντα κανονισμό και τη συμφωνία υποδοχής και χρήσης καθορίζεται στη γραπτή συμφωνία κοινοπραξίας που αναφέρεται στην παράγραφο 3.***

***6. Ένα κράτος μέλος μπορεί να προσχωρήσει σε υφιστάμενη κοινοπραξία υποδοχής με τη σύμφωνη γνώμη των μελών της κοινοπραξίας υποδοχής. Η γραπτή συμφωνία κοινοπραξίας που αναφέρεται στην παράγραφο 3 και η συμφωνία υποδοχής και χρήσης τροποποιούνται αναλόγως. Αυτό δεν θίγει τα δικαιώματα κυριότητας του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας («ΕΚΑΚ») επί των εργαλείων, των υποδομών ή των υπηρεσιών που έχουν ήδη αποκτηθεί από κοινού με την εν λόγω κοινοπραξία υποδοχής.***

Άρθρο 6

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

1. Τα μέλη μιας κοινοπραξίας υποδοχής ***διασφαλίζουν ότι οι εθνικοί τους κυβερνοκόμβοι ανταλλάσσουν, στο πλαίσιο της γραπτής συμφωνίας κοινοπραξίας που αναφέρεται στο άρθρο 5 παράγραφος 3, σχετικές πληροφορίες, ανωνυμοποιημένες κατά περίπτωση, όπως πληροφορίες*** 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 ανίχνευση κυβερνοεπιθέσεων, ***μεταξύ τους και εντός του διασυνοριακού κυβερνοκόμβου,*** στον βαθμό που η εν λόγω ανταλλαγή πληροφοριών:

   α) ***προωθεί και ενισχύει την ανίχνευση κυβερνοαπειλών και ενισχύει τις ικανότητες του δικτύου CSIRT για την πρόληψη και την αντιμετώπιση περιστατικών ή τον μετριασμό των επιπτώσεών τους·***

   β) ενισχύει το επίπεδο της κυβερνοασφάλειας, ***για παράδειγμα*** 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, των σταδίων αντιμετώπισης και ανάκαμψης ή της προώθησης της συνεργατικής έρευνας για τις απειλές μεταξύ δημόσιων και ιδιωτικών οντοτήτων.

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

α) δέσμευση για ανταλλαγή***, μεταξύ των μελών της κοινοπραξίας, των πληροφοριών*** που αναφέρονται στην παράγραφο 1 και οι προϋποθέσεις υπό τις οποίες πρέπει να ανταλλάσσονται τα εν λόγω δεδομένα και πληροφορίες·

β) ***πλαίσιο διακυβέρνησης που αποσαφηνίζει και παρέχει κίνητρα για την ανταλλαγή από όλους τους συμμετέχοντες των σχετικών πληροφοριών, ανωνυμοποιημένων κατά περίπτωση, όπως αναφέρονται στην παράγραφο 1·***

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

***Η γραπτή συμφωνία κοινοπραξίας μπορεί να ορίζει ότι οι πληροφορίες που αναφέρονται στην παράγραφο 1 πρέπει να ανταλλάσσονται σύμφωνα με το ενωσιακό και το εθνικό δίκαιο.***

***3. Οι διασυνοριακοί κυβερνοκόμβοι συνάπτουν μεταξύ τους συμφωνίες συνεργασίας, στις οποίες καθορίζονται οι αρχές διαλειτουργικότητας και ανταλλαγής πληροφοριών μεταξύ των διασυνοριακών κυβερνοκόμβων. Οι διασυνοριακοί κυβερνοκόμβοι ενημερώνουν την Επιτροπή σχετικά με τις συμφωνίες συνεργασίας που συνάπτονται.***

4. ***Η ανταλλαγή πληροφοριών, όπως αναφέρεται στην παράγραφο 1, μεταξύ διασυνοριακών κυβερνοκόμβων διασφαλίζεται χάρη σε ένα υψηλό επίπεδο διαλειτουργικότητας. Για τη στήριξη της εν λόγω διαλειτουργικότητας, ο ENISA εκδίδει, σε στενή διαβούλευση με την Επιτροπή, χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση έως … [12 μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού] κατευθυντήριες γραμμές για τη διαλειτουργικότητα, προσδιορίζοντας ιδίως μορφότυπους και πρωτόκολλα ανταλλαγής πληροφοριών, και λαμβάνοντας υπόψη τα διεθνή πρότυπα και τις βέλτιστες πρακτικές, καθώς και τη λειτουργία τυχόν ήδη συσταθέντων διασυνοριακών κυβερνοκόμβων. Οι απαιτήσεις διαλειτουργικότητας που προβλέπονται για τις συμφωνίες συνεργασίας των διασυνοριακών κυβερνοκόμβων βασίζονται στις κατευθυντήριες γραμμές που εκδίδει ο ENISA.***

Άρθρο 7

Συνεργασία και ανταλλαγή πληροφοριών με ***δίκτυα σε επίπεδο Ένωσης***

***1.*** ***Οι διασυνοριακοί κυβερνοκόμβοι και το δίκτυο CSIRT συνεργάζονται στενά, ιδίως με στόχο την ανταλλαγή πληροφοριών. Για τον σκοπό αυτό, συμφωνούν επί διαδικαστικών ρυθμίσεων όσον αφορά τη συνεργασία και την ανταλλαγή σχετικών πληροφοριών και, με την επιφύλαξη της παραγράφου 2, όσον αφορά τα είδη των πληροφοριών που πρέπει να ανταλλάσσονται.***

2. ***Όταν οι διασυνοριακοί κυβερνοκόμβοι λαμβάνουν πληροφορίες σχετικά με δυνητικό ή εξελισσόμενο περιστατικό κυβερνοασφάλειας μεγάλης κλίμακας, διασφαλίζουν, για τους σκοπούς της κοινής αντίληψης της κατάστασης, ότι παρέχονται σχετικές πληροφορίες καθώς και έγκαιρες προειδοποιήσεις στις αρχές των κρατών μελών και στην Επιτροπή μέσω του EU-CyCLONe και του δικτύου CSIRT, χωρίς αδικαιολόγητη καθυστέρηση.***

Άρθρο 8

Ασφάλεια

1. Τα κράτη μέλη που συμμετέχουν ***στο ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια*** διασφαλίζουν υψηλό επίπεδο ***κυβερνοασφάλειας, συμπεριλαμβανομένων της εμπιστευτικότητας και της*** ασφάλειας των δεδομένων***, καθώς*** και υλικής ασφάλειας ***του δικτύου του ευρωπαϊκού συστήματος προειδοποίησης για την κυβερνοασφάλεια***, και μεριμνούν για την κατάλληλη διαχείριση και έλεγχο ***του δικτύου*** ώστε να προστατεύεται από απειλές και να διασφαλίζεται η ασφάλειά ***του*** και η ασφάλεια των συστημάτων, συμπεριλαμβανομένης της ασφάλειας ***των δεδομένων και των πληροφοριών*** που ανταλλάσσονται μέσω ***του δικτύου***.

2. ***Τα κράτη μέλη που συμμετέχουν στο ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια διασφαλίζουν ότι η ανταλλαγή πληροφοριών που αναφέρεται στο άρθρο 6 παράγραφος 1, στο πλαίσιο του ευρωπαϊκού συστήματος προειδοποίησης για την κυβερνοασφάλεια, με οποιαδήποτε οντότητα εκτός των δημόσιων αρχών ή φορέων κράτους μέλους δεν επηρεάζει αρνητικά τα συμφέροντα ασφάλειας της Ένωσης ή των κρατών μελών.***

*Άρθρο 9*

*Χρηματοδότηση του ευρωπαϊκού συστήματος προειδοποίησης για την κυβερνοασφάλεια*

***1.*** ***Κατόπιν πρόσκλησης εκδήλωσης ενδιαφέροντος των κρατών μελών που προτίθενται να συμμετάσχουν στο ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια, το ΕΚΑΚ επιλέγει τα κράτη μέλη που θα συμμετάσχουν, μαζί με το ΕΚΑΚ, σε κοινή διαδικασία προμήθειας εργαλείων, υποδομών ή υπηρεσιών, με σκοπό τη δημιουργία, ή την ενίσχυση των ικανοτήτων, εθνικών κυβερνοκόμβων που έχουν οριστεί ή συσταθεί δυνάμει του άρθρου 4 παράγραφος 1. Το ΕΚΑΚ μπορεί να χορηγεί επιχορηγήσεις στα επιλεγμένα κράτη μέλη για τη χρηματοδότηση της λειτουργίας των εν λόγω εργαλείων, υποδομών ή υπηρεσιών. Η χρηματοδοτική συνεισφορά της Ένωσης καλύπτει έως και το 50 % του κόστους αγοράς των εργαλείων, υποδομών ή υπηρεσιών, και έως το 50 % του κόστους λειτουργίας. Το επιλεγμένο κράτος μέλος καλύπτει το υπόλοιπο κόστος. Πριν από την έναρξη της διαδικασίας αγοράς των εργαλείων, υποδομών ή υπηρεσιών, το ΕΚΑΚ και το επιλεγμένο κράτος μέλος συνάπτουν συμφωνία υποδοχής και χρήσης που ρυθμίζει τη χρήση των εργαλείων, υποδομών ή υπηρεσιών.**

*2. Εάν ο εθνικός κυβερνοκόμβος ενός κράτους μέλους δεν συμμετέχει σε διασυνοριακό κυβερνοκόμβο εντός δύο ετών από την ημερομηνία κατά την οποία αποκτήθηκαν τα εργαλεία, οι υποδομές ή οι υπηρεσίες ή κατά την οποία ελήφθη χρηματοδότηση μέσω επιχορηγήσεων, όποιο από τα δύο συνέβη νωρίτερα, το εν λόγω κράτος μέλος δεν θα είναι επιλέξιμο για πρόσθετη ενωσιακή στήριξη δυνάμει του παρόντος κεφαλαίου, μέχρι να συμμετάσχει σε διασυνοριακό κυβερνοκόμβο.*

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

***4. Το ΕΚΑΚ διενεργεί, τουλάχιστον ανά διετία, χαρτογράφηση των εργαλείων, των υποδομών ή των υπηρεσιών που είναι αναγκαία και επαρκούς ποιότητας για τη δημιουργία, ή την ενίσχυση των ικανοτήτων, εθνικών κυβερνοκόμβων και διασυνοριακών κυβερνοκόμβων, καθώς και της διαθεσιμότητάς τους, μεταξύ άλλων από νομικές οντότητες που είναι εγκατεστημένες ή θεωρείται ότι είναι εγκατεστημένες σε κράτη μέλη και ελέγχονται από κράτη μέλη ή από υπηκόους των κρατών μελών. Κατά την προετοιμασία της χαρτογράφησης, το ΕΚΑΚ συμβουλεύεται το δίκτυο CSIRT, τυχόν υφιστάμενους διασυνοριακούς κυβερνοκόμβους, τον ENISA και την Επιτροπή.***

Κεφάλαιο III

ΜΗΧΑΝΙΣΜΟΣ ΕΚΤΑΚΤΗΣ ΑΝΑΓΚΗΣ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Άρθρο 10

Θέσπιση του μηχανισμού έκτακτης ανάγκης για την κυβερνοασφάλεια

1. Θεσπίζεται μηχανισμός έκτακτης ανάγκης ***για την κυβερνοασφάλεια*** με σκοπό ***τη στήριξη της βελτίωσης*** της ανθεκτικότητας της Ένωσης σε ***κυβερνοαπειλές*** και την προετοιμασία και τον μετριασμό, σε πνεύμα αλληλεγγύης, των βραχυπρόθεσμων επιπτώσεων σημαντικών ***περιστατικών κυβερνοασφάλειας, περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας, και περιστατικών ισοδύναμων με περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας***.

***2. Στην περίπτωση των κρατών μελών, οι δράσεις που προβλέπονται στο πλαίσιο του μηχανισμού έκτακτης ανάγκης για την κυβερνοασφάλεια παρέχονται κατόπιν αιτήματος και είναι συμπληρωματικές προς τις προσπάθειες και τις δράσεις των κρατών μελών για την προετοιμασία, την αντιμετώπιση και την ανάκαμψη σε σχέση με περιστατικά.***

3. Οι δράσεις για την υλοποίηση του ***μηχανισμού έκτακτης ανάγκης για την κυβερνοασφάλεια*** στηρίζονται με χρηματοδότηση από ***το πρόγραμμα «Ψηφιακή Ευρώπη»*** και υλοποιούνται σύμφωνα με τον κανονισμό (ΕΕ) 2021/694, και ιδίως τον ειδικό στόχο 3.

*4.* ***Οι δράσεις στο πλαίσιο του μηχανισμού έκτακτης ανάγκης για την κυβερνοασφάλεια εκτελούνται πρωτίστως μέσω του ΕΚΑΚ σύμφωνα με τον κανονισμό (ΕΕ) 2021/887. Εν τούτοις, δράσεις για την υλοποίηση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας όπως αναφέρονται στο άρθρο 11 στοιχείο β) του παρόντος κανονισμού υλοποιούνται από την Επιτροπή και τον ENISA.***

Άρθρο 11

Είδος δράσεων

Ο μηχανισμός ***έκτακτης ανάγκης για την κυβερνοασφάλεια*** στηρίζει τα ακόλουθα είδη δράσεων:

α) δράσεις ετοιμότητας, ***και συγκεκριμένα:***

***i) συντονισμένες δοκιμές ετοιμότητας οντοτήτων που δραστηριοποιούνται σε τομείς υψηλής κρισιμότητας σε ολόκληρη την Ένωση, όπως ορίζονται στο άρθρο 12·***

***ii) άλλες δράσεις ετοιμότητας για οντότητες που δραστηριοποιούνται σε τομείς υψηλής κρισιμότητας ή οντότητες που δραστηριοποιούνται σε άλλους κρίσιμους τομείς, όπως ορίζονται στο άρθρο 13·***

β) ***δράσεις που στηρίζουν την αντιμετώπιση σημαντικών περιστατικών κυβερνοασφάλειας, περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας, και περιστατικών ισοδύναμων με περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας, και την αρχική 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 14·***

γ) δράσεις στήριξης της αμοιβαίας συνδρομής***, όπως αναφέρονται στο άρθρο 18***.

Άρθρο 12

Συντονισμένες δοκιμές ετοιμότητας οντοτήτων

***1. Ο μηχανισμός έκτακτης ανάγκης για την κυβερνοασφάλεια στηρίζει τις εθελοντικές συντονισμένες δοκιμές ετοιμότητας οντοτήτων που δραστηριοποιούνται σε τομείς υψηλής κρισιμότητας.***

***2. Οι συντονισμένες δοκιμές ετοιμότητας μπορεί να συνίστανται σε δραστηριότητες ετοιμότητας, όπως δοκιμές διείσδυσης, και στην αξιολόγηση απειλών.***

***3. Η στήριξη για δράσεις ετοιμότητας δυνάμει του παρόντος άρθρου παρέχεται στα κράτη μέλη πρωτίστως με τη μορφή επιχορηγήσεων και υπό τους όρους που καθορίζονται στα σχετικά προγράμματα εργασίας όπως αναφέρονται στο άρθρο 24 του κανονισμού (ΕΕ) 2021/694.***

4. Για τους σκοπούς της στήριξης των συντονισμένων δοκιμών ετοιμότητας των οντοτήτων που αναφέρονται στο άρθρο 11 παράγραφος 1 στοιχείο α) ***σημείο i)*** του παρόντος κανονισμού, σε ολόκληρη την Ένωση, η Επιτροπή, αφού ζητήσει τη γνώμη της ομάδας συνεργασίας NIS***, του EU-CyCLONe*** και του ENISA, προσδιορίζει τους σχετικούς τομείς ή υποτομείς από τους τομείς υψηλής κρισιμότητας που παρατίθενται στο παράρτημα I της οδηγίας (ΕΕ) 2022/2555, ***για τους οποίους μπορεί να εκδοθεί πρόσκληση υποβολής προτάσεων για τη χορήγηση επιχορηγήσεων***. ***Η συμμετοχή των κρατών μελών στην εν λόγω υποβολή προτάσεων είναι προαιρετική.***

***5. Κατά τον προσδιορισμό των τομέων ή υποτομέων που αναφέρονται στην παράγραφο 4, η Επιτροπή λαμβάνει υπόψη τις συντονισμένες εκτιμήσεις κινδύνου και τις δοκιμές ανθεκτικότητας σε επίπεδο Ένωσης, καθώς και τα αποτελέσματά τους.***

6. ***Η ομάδα συνεργασίας NIS, σε συνεργασία με την Επιτροπή, τον ύπατο εκπρόσωπο της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας («ύπατος εκπρόσωπος») και τον ENISA, και, στο πλαίσιο της εντολής του, το EU-CyCLONe, αναπτύσσει κοινά σενάρια κινδύνου και μεθοδολογίες για τις συντονισμένες δοκιμές ετοιμότητας που αναφέρονται στο άρθρο 11 στοιχείο α) σημείο i) και, κατά περίπτωση, για άλλες δράσεις ετοιμότητας που αναφέρονται στο στοιχείο α) σημείο ii) του εν λόγω άρθρου.***

*7.* ***Όταν μια οντότητα που δραστηριοποιείται σε τομέα υψηλής κρισιμότητας συμμετέχει εθελοντικά σε συντονισμένες δοκιμές ετοιμότητας και οι εν λόγω δοκιμές οδηγούν σε συστάσεις ειδικών μέτρων, οι οποίες μπορούν να ενσωματωθούν από τη συμμετέχουσα οντότητα σε σχέδιο αποκατάστασης, η αρχή του κράτους μέλους που είναι υπεύθυνη για τη διενέργεια των συντονισμένων δοκιμών ετοιμότητας επανεξετάζει, κατά περίπτωση, την επακολούθηση των εν λόγω μέτρων από τις συμμετέχουσες οντότητες με σκοπό την ενίσχυση της ετοιμότητας.***

*Άρθρο 13*

*Άλλες δράσεις ετοιμότητας*

***1.*** ***Ο μηχανισμός έκτακτης ανάγκης για την κυβερνοασφάλεια στηρίζει επίσης δράσεις ετοιμότητας που δεν καλύπτονται από το άρθρο 12. Οι εν λόγω δράσεις περιλαμβάνουν δράσεις ετοιμότητας για οντότητες σε τομείς που δεν προσδιορίζονται σε σχέση με τις συντονισμένες δοκιμές ετοιμότητας σύμφωνα με το άρθρο 12. Οι δράσεις αυτές μπορούν να στηρίζουν την παρακολούθηση ευπαθειών, την παρακολούθηση κινδύνων, ασκήσεις και προγράμματα κατάρτισης.***

***2.*** ***Η στήριξη για δράσεις ετοιμότητας δυνάμει του παρόντος άρθρου παρέχεται στα κράτη μέλη κατόπιν αιτήματος και πρωτίστως με τη μορφή επιχορηγήσεων και υπό τους όρους που καθορίζονται στα σχετικά προγράμματα εργασίας όπως αναφέρονται στο άρθρο 24 του κανονισμού (ΕΕ) 2021/694.***

Άρθρο 14

Σύσταση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας

1. Δημιουργείται εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, με σκοπό να βοηθά***, κατόπιν αιτήματος,*** τους χρήστες όπως αναφέρονται στην παράγραφο 3 να αντιμετωπίζουν ή να παρέχουν στήριξη για την αντιμετώπιση σημαντικών ***περιστατικών κυβερνοασφάλειας, περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας, και περιστατικών ισοδύναμων με περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας,*** και την ***αρχική*** ανάκαμψη από τέτοια περιστατικά.

2. Η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας συνίσταται σε υπηρεσίες αντιμετώπισης ▌ από αξιόπιστους παρόχους ***διαχειριζόμενων υπηρεσιών ασφάλειας*** που επιλέγονται σύμφωνα με τα κριτήρια που ορίζονται στο άρθρο 17 παράγραφος 2. Η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας ***μπορεί να*** περιλαμβάνει προδεσμευμένες υπηρεσίες. ***Οι προδεσμευμένες υπηρεσίες ενός αξιόπιστου παρόχου διαχειριζόμενων υπηρεσιών ασφάλειας μπορούν να μετατρέπονται σε υπηρεσίες ετοιμότητας που σχετίζονται με την πρόληψη και την αντιμετώπιση περιστατικών, στις περιπτώσεις που οι εν λόγω προδεσμευμένες υπηρεσίες δεν χρησιμοποιούνται για την αντιμετώπιση περιστατικών κατά τη διάρκεια του χρονικού διαστήματος για το οποίο οι εν λόγω υπηρεσίες είναι προδεσμευμένες,. Η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας μπορεί να αναπτύσσεται κατόπιν αιτήματος σε όλα τα κράτη μέλη, τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης και σε τρίτες χώρες συνδεδεμένες με το*** πρόγραμμα «Ψηφιακή Ευρώπη» ***όπως αναφέρονται στο άρθρο 17 παράγραφος 1.***

3. ***Οι χρήστες των υπηρεσιών που προβλέπονται από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας είναι οι εξής:***

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

β) ***η CERT-ΕΕ, σύμφωνα με το άρθρο 13 του κανονισμού (ΕΕ, Ευρατόμ) 2023/2841***·

***γ) αρμόδιες αρχές, όπως οι ομάδες αντιμετώπισης περιστατικών ασφάλειας υπολογιστών και οι αρχές διαχείρισης κρίσεων στον κυβερνοχώρο των τρίτων χωρών συνδεδεμένων με το*** πρόγραμμα «Ψηφιακή Ευρώπη» ***σύμφωνα με το άρθρο 19 παράγραφος 8.***

4. 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 συνεργασίας NIS*** και σύμφωνα με τις απαιτήσεις των χρηστών που αναφέρονται στην παράγραφο 3, και 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. ***Οι προτεραιότητες αυτές επανεξετάζονται και, κατά περίπτωση, αναθεωρούνται ανά διετία. Η Επιτροπή ενημερώνει το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο σχετικά με τις προτεραιότητες αυτές και τις αναθεωρήσεις τους.***

5. ***Με την επιφύλαξη της συνολικής ευθύνης της Επιτροπής για την υλοποίηση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας που αναφέρεται στην παράγραφο 4 του παρόντος άρθρου, και με την επιφύλαξη συμφωνίας συνεισφοράς, όπως ορίζεται στο άρθρο 2 σημείο 19) του κανονισμού (ΕΕ, Ευρατόμ) 2024/2509, η Επιτροπή αναθέτει τη λειτουργία και τη διαχείριση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, εν όλω ή εν μέρει, στον ENISA. Οι πτυχές που δεν ανατίθενται στον ENISA εξακολουθούν να υπόκεινται σε άμεση διαχείριση από την Επιτροπή.***

6. ***Ο ENISA διενεργεί, τουλάχιστον ανά διετία, χαρτογράφηση των υπηρεσιών που χρειάζονται οι χρήστες που αναφέρονται στην παράγραφο 3 στοιχεία α) και β) του παρόντος άρθρου. Η χαρτογράφηση περιλαμβάνει επίσης τη διαθεσιμότητα των υπηρεσιών αυτών, μεταξύ άλλων από νομικές οντότητες που είναι ή θεωρούνται εγκατεστημένες σε κράτη μέλη και ελέγχονται από κράτη μέλη ή από υπηκόους κρατών μελών. Κατά τη χαρτογράφηση της εν λόγω διαθεσιμότητας, ο ENISA αξιολογεί τις δεξιότητες και την ικανότητα του εργατικού δυναμικού της Ένωσης στον τομέα της κυβερνοασφάλειας σε σχέση με τους στόχους της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. Κατά τη διενέργεια της χαρτογράφησης, ο ENISA διαβουλεύεται με την ομάδα συνεργασίας NIS, το EU-CyCLONe, την Επιτροπή και, κατά περίπτωση, το διοργανικό συμβούλιο κυβερνοασφάλειας που θεσπίστηκε δυνάμει του άρθρου 10 του κανονισμού (ΕΕ, Ευρατόμ) 2023/2841 (ΙΙCB). Κατά τη χαρτογράφηση της διαθεσιμότητας των υπηρεσιών, ο ENISA διαβουλεύεται επίσης με τα σχετικά ενδιαφερόμενα μέρη του κλάδου της κυβερνοασφάλειας, συμπεριλαμβανομένων των παρόχων διαχειριζόμενων υπηρεσιών ασφάλειας. Ο ENISA διενεργεί παρόμοια χαρτογράφηση, αφού ενημερώσει το Συμβούλιο και ζητήσει τη γνώμη του EU-CyCLONe και της Επιτροπής και, κατά περίπτωση, του ύπατου εκπροσώπου, για τον προσδιορισμό των αναγκών των χρηστών που αναφέρονται στην παράγραφο 3 στοιχείο γ) του παρόντος άρθρου.***

7. ***Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις σύμφωνα με το άρθρο 23 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. ***Κατά την κατάρτιση των εν λόγω κατ' εξουσιοδότηση πράξεων, η Επιτροπή λαμβάνει υπόψη τη χαρτογράφηση που αναφέρεται στην παράγραφο 6 του παρόντος άρθρου και μπορεί να ανταλλάσσει συμβουλές και να συνεργάζεται με την ομάδα συνεργασίας NIS και τον ENISA.***

Άρθρο 15

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 ***αρχικής*** ανάκαμψης από σημαντικά ***περιστατικά κυβερνοασφάλειας, περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας, και περιστατικά ισοδύναμα με περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας***.

2. Για να λάβουν στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, οι χρήστες που αναφέρονται στο άρθρο 14 παράγραφος 3 λαμβάνουν ***όλα τα κατάλληλα*** μέτρα για τον μετριασμό των επιπτώσεων του περιστατικού για το οποίο ζητείται η στήριξη, συμπεριλαμβανομένης***, κατά περίπτωση,*** της παροχής άμεσης τεχνικής βοήθειας, και άλλων πόρων για να βοηθήσουν στην αντιμετώπιση του περιστατικού, καθώς και προσπαθειών ▌ ανάκαμψης.

3. ***Τα αιτήματα στήριξης διαβιβάζονται στην αναθέτουσα αρχή ως εξής:***

***α) στην περίπτωση των χρηστών που αναφέρονται στο άρθρο 14 παράγραφος 3 στοιχείο α) του παρόντος κανονισμού, μέσω του ενιαίου σημείου επαφής που ορίζεται ή θεσπίζεται δυνάμει του άρθρου 8 παράγραφος 3 της οδηγίας (ΕΕ) 2022/2555·***

***β) στην περίπτωση του χρήστη που αναφέρεται στο άρθρο 14 παράγραφος 3 στοιχείο β), από τον εν λόγω χρήστη·***

***γ) στην περίπτωση των χρηστών που αναφέρονται στο άρθρο 14 παράγραφος 3 στοιχείο γ), μέσω του ενιαίου σημείου επαφής που αναφέρεται στο άρθρο 19 παράγραφος 9.***

4. ***Στην περίπτωση αιτημάτων από χρήστες που αναφέρονται στο άρθρο 14 παράγραφος 3 στοιχείο α) του παρόντος κανονισμού,*** τα κράτη μέλη ενημερώνουν το δίκτυο CSIRT και, κατά περίπτωση, το EU-CyCLONe σχετικά με τα αιτήματα ***των χρηστών τους*** για στήριξη της αντιμετώπισης περιστατικών και της ***αρχικής*** ανάκαμψης από αυτά σύμφωνα με το παρόν άρθρο.

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

α) κατάλληλες πληροφορίες σχετικά με την επηρεαζόμενη οντότητα και τις δυνητικές επιπτώσεις του περιστατικού ***στα εξής:***

***i) στην περίπτωση των χρηστών που αναφέρονται στο άρθρο 14 παράγραφος 3 στοιχείο α), στα επηρεαζόμενα κράτη μέλη και τους επηρεαζόμενους χρήστες, συμπεριλαμβανομένου του κινδύνου δευτερογενών επιπτώσεων σε άλλο κράτος μέλος·***

***ii) στην περίπτωση του χρήστη που αναφέρεται στο άρθρο 14 παράγραφος 3 στοιχείο β), στα επηρεαζόμενα θεσμικά και λοιπά όργανα ή οργανισμούς της Ένωσης·***

***iii) στην περίπτωση των χρηστών που αναφέρονται στο άρθρο 14 παράγραφος 3 στοιχείο γ), στις επηρεαζόμενες συνδεδεμένες με το*** πρόγραμμα «Ψηφιακή Ευρώπη» ***χώρες·***

***β) πληροφορίες σχετικά με τη ζητούμενη υπηρεσία, μαζί με την προγραμματισμένη χρήση της ζητούμενης στήριξης, συμπεριλαμβανομένης αναφοράς των εκτιμώμενων αναγκών·***

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

δ) ***κατά περίπτωση, διαθέσιμες*** πληροφορίες σχετικά με άλλες μορφές στήριξης που έχει στη διάθεσή της η επηρεαζόμενη οντότητα ▌.

6. Ο ENISA, σε συνεργασία με την Επιτροπή και ***το EU-CyCLONe***, καταρτίζει υπόδειγμα για τη διευκόλυνση της υποβολής αιτημάτων στήριξης από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας.

7. ***Η Επιτροπή μπορεί, μέσω εκτελεστικών πράξεων, να προσδιορίσει περαιτέρω τις λεπτομερείς διαδικαστικές ρυθμίσεις για τον τρόπο με τον οποίο υποβάλλονται και αντιμετωπίζονται τα αιτήματα για υπηρεσίες στήριξης της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας σύμφωνα με το παρόν άρθρο, το άρθρο 16 παράγραφος 1 και το άρθρο 19 παράγραφος 10, συμπεριλαμβανομένων ρυθμίσεων για την υποβολή των εν λόγω αιτημάτων και την παροχή των απαντήσεων και των υποδειγμάτων για τις εκθέσεις που αναφέρονται στο άρθρο 16 παράγραφος 9.*** Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης στην οποία παραπέμπει το άρθρο 24 παράγραφος 2.

Άρθρο 16

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

***1. Στην περίπτωση αιτημάτων από χρήστες που αναφέρονται στο άρθρο 14 παράγραφος 3 στοιχεία α) και β), τα αιτήματα στήριξης από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας αξιολογούνται από την αναθέτουσα αρχή. Διαβιβάζεται απάντηση στους χρήστες που αναφέρονται στο άρθρο 14 παράγραφος 3 στοιχεία α) και β) χωρίς καθυστέρηση και σε κάθε περίπτωση το αργότερο εντός 48 ωρών από την υποβολή του αιτήματος, προκειμένου να διασφαλιστεί η αποτελεσματικότητα της στήριξης. Η αναθέτουσα αρχή ενημερώνει το Συμβούλιο και την Επιτροπή για τα αποτελέσματα της διαδικασίας.***

***2. Όσον αφορά τις πληροφορίες που ανταλλάσσονται κατά την υποβολή αιτήματος και την παροχή των υπηρεσιών της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, όλα τα μέρη που συμμετέχουν στην εφαρμογή του παρόντος κανονισμού:***

***α) περιορίζουν τη χρήση και την ανταλλαγή των εν λόγω πληροφοριών σε ό,τι είναι αναγκαίο για την εκπλήρωση των υποχρεώσεων ή των καθηκόντων τους δυνάμει του παρόντος κανονισμού·***

***β) χρησιμοποιούν και ανταλλάσσουν τις τυχόν πληροφορίες που είναι εμπιστευτικές ή διαβαθμισμένες σύμφωνα με το ενωσιακό και το εθνικό δίκαιο, μόνο κατά τρόπο που είναι σύμφωνος με το εν λόγω δίκαιο· και***

***γ) διασφαλίζουν την αποτελεσματική, αποδοτική και ασφαλή ανταλλαγή πληροφοριών, κατά περίπτωση χρησιμοποιώντας και τηρώντας σχετικά πρωτόκολλα ανταλλαγής πληροφοριών, συμπεριλαμβανομένου του πρωτοκόλλου φωτεινού σηματοδότη.***

3. ***Κατά την αξιολόγηση των επιμέρους αιτημάτων σύμφωνα με το άρθρο 16 παράγραφος 1 και το άρθρο 19 παράγραφος 10, η αναθέτουσα αρχή ή η Επιτροπή, κατά περίπτωση, αξιολογεί πρώτα κατά πόσον πληρούνται τα κριτήρια που αναφέρονται στο άρθρο 15 παράγραφοι 1 και 2. Στην περίπτωση αυτή, αξιολογούν τη διάρκεια και τη φύση της στήριξης που είναι κατάλληλη, λαμβάνοντας υπόψη τον στόχο που αναφέρεται στο άρθρο 1 παράγραφος 3 στοιχείο β) και τα ακόλουθα κριτήρια, κατά περίπτωση:***

α) ***την κλίμακα και τη*** σοβαρότητα του περιστατικού κυβερνοασφάλειας·

β) τον τύπο της επηρεαζόμενης οντότητας, με υψηλότερη προτεραιότητα σε περιστατικά που επηρεάζουν βασικές οντότητες, όπως αναφέρονται στο άρθρο 3 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555·

γ) ***τις δυνητικές επιπτώσεις του περιστατικού στα επηρεαζόμενα κράτη μέλη, θεσμικά και λοιπά όργανα ή οργανισμούς της Ένωσης, ή τρίτες χώρες συνδεδεμένες με το*** πρόγραμμα «Ψηφιακή Ευρώπη»·

δ) ***τον δυνητικό διασυνοριακό χαρακτήρα του περιστατικού και τον κίνδυνο πρόκλησης δευτερογενών επιπτώσεων σε άλλα κράτη μέλη, θεσμικά και λοιπά όργανα ή οργανισμούς της Ένωσης, ή τρίτες χώρες συνδεδεμένες με το*** πρόγραμμα «Ψηφιακή Ευρώπη»·

ε) τα μέτρα που λαμβάνονται από τον χρήστη για την υποβοήθηση της αντιμετώπισης και τις προσπάθειες ***αρχικής*** ανάκαμψης, όπως αναφέρονται στο άρθρο 15 παράγραφος 2.

***4. Για την ιεράρχηση των αιτημάτων, στην περίπτωση παράλληλων αιτημάτων από χρήστες που αναφέρονται στο άρθρο 14 παράγραφος 3, τα κριτήρια που αναφέρονται στην παράγραφο 3 του παρόντος άρθρου λαμβάνονται υπόψη, κατά περίπτωση, με την επιφύλαξη της αρχής της καλόπιστης συνεργασίας μεταξύ των κρατών μελών και των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης. Όταν δύο ή περισσότερα αιτήματα αξιολογούνται ως ισότιμα βάσει των εν λόγω κριτηρίων που αναφέρονται στην παράγραφο 2, δίνεται υψηλότερη προτεραιότητα στα αιτήματα των χρηστών των κρατών μελών. Όταν η λειτουργία και η διαχείριση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας έχει ανατεθεί, εν όλω ή εν μέρει, στον ENISA δυνάμει του άρθρου 14 παράγραφος 5, ο ENISA και η Επιτροπή συνεργάζονται στενά για την ιεράρχηση των αιτημάτων σύμφωνα με την παρούσα παράγραφο.***

5. Οι υπηρεσίες εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας παρέχονται σύμφωνα με ειδικές συμφωνίες μεταξύ του ***αξιόπιστου*** παρόχου διαχειριζόμενων υπηρεσιών ασφάλειας και του χρήστη στον οποίο παρέχεται η στήριξη στο πλαίσιο της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. ***Οι εν λόγω υπηρεσίες μπορούν να παρέχονται σύμφωνα με ειδικές συμφωνίες μεταξύ του αξιόπιστου παρόχου διαχειριζόμενων υπηρεσιών ασφάλειας, του χρήστη και της επηρεαζόμενης οντότητας. Όλες οι συμφωνίες που αναφέρονται στην παρούσα παράγραφο περιλαμβάνουν, μεταξύ άλλων, όρους ευθύνης.***

6. Οι συμφωνίες που αναφέρονται στην παράγραφο 5 ▌ 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***.

7. Η Επιτροπή***, ο ENISA και οι χρήστες της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας*** δεν φέρουν συμβατική ευθύνη για ζημία που προκαλείται σε τρίτους από τις υπηρεσίες που παρέχονται στο πλαίσιο της υλοποίησης της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας.

***8. Οι χρήστες μπορούν να χρησιμοποιούν τις υπηρεσίες εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας που παρέχονται ως απάντηση σε αίτημα δυνάμει του άρθρου 15 παράγραφος 1 μόνο για τη στήριξη της αντιμετώπισης σημαντικών περιστατικών κυβερνοασφάλειας, περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας, και περιστατικών ισοδύναμων με περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας, και την αρχική ανάκαμψη από αυτά. Μπορούν να χρησιμοποιούν τις υπηρεσίες αυτές μόνο σε σχέση με τα εξής:***

***α) οντότητες που δραστηριοποιούνται σε τομείς υψηλής κρισιμότητας ή οντότητες που δραστηριοποιούνται σε άλλους κρίσιμους τομείς, στην περίπτωση των χρηστών που αναφέρονται στο άρθρο 14 παράγραφος 3 στοιχείο α), και ισοδύναμες οντότητες στην περίπτωση των χρηστών που αναφέρονται στο άρθρο 14 παράγραφος 3 στοιχείο γ)· και***

***β) θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης, στην περίπτωση του χρήστη που αναφέρεται στο άρθρο 14 παράγραφος 3 στοιχείο β).***

9. Εντός ***δύο μηνών*** από το τέλος της στήριξης, ***χρήστες που έχουν λάβει στήριξη υποβάλλουν*** συνοπτική έκθεση σχετικά με την παρασχεθείσα υπηρεσία, τα αποτελέσματα που επιτεύχθηκαν και τα διδάγματα που αντλήθηκαν***, προς:***

***α) την Επιτροπή, τον ENISA, το δίκτυο CSIRT και το EU-CyCLONe, στην περίπτωση χρηστών που αναφέρονται στο άρθρο 14 παράγραφος 3 στοιχείο α)·***

***β) την Επιτροπή, τον ENISA και το IICB, στην περίπτωση του χρήστη που αναφέρεται στο άρθρο 14 παράγραφος 3 στοιχείο β)·***

***γ) την Επιτροπή, στην περίπτωση χρηστών που αναφέρονται στο άρθρο 14 παράγραφος 3 στοιχείο γ).***

***Η Επιτροπή διαβιβάζει κάθε συνοπτική έκθεση που λαμβάνει από χρήστες που αναφέρονται στο άρθρο 14 παράγραφος 3 δυνάμει του πρώτου εδαφίου στοιχείο γ)της παρούσας παραγράφου, στο Συμβούλιο και στον ύπατο εκπρόσωπο.***

***10.*** ***Όταν η λειτουργία και η διαχείριση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας έχει ανατεθεί, εν όλω ή εν μέρει, στον ENISA δυνάμει του άρθρου 14 παράγραφος 5 του παρόντος κανονισμού, ο ENISA υποβάλλει σχετικές εκθέσεις στην Επιτροπή και τη συμβουλεύεται σε τακτική βάση όσον αφορά το θέμα αυτό. Στο πλαίσιο αυτό, ο ENISA διαβιβάζει αμέσως στην Επιτροπή τυχόν αιτήματα που λαμβάνει από τους χρήστες που αναφέρονται στο άρθρο 14 παράγραφος 3 στοιχείο γ) του παρόντος κανονισμού και, όταν απαιτείται για τους σκοπούς της ιεράρχησης βάσει του παρόντος άρθρου, τυχόν αιτήματα που έχει λάβει από χρήστες που αναφέρονται στο άρθρο 14 παράγραφος 3 στοιχείο α) ή β) του παρόντος κανονισμού. Οι υποχρεώσεις της παρούσας παραγράφου ισχύουν με την επιφύλαξη του άρθρου 14 του κανονισμού (ΕΕ) 2019/881.***

11. ***Στην περίπτωση των χρηστών που αναφέρονται στο άρθρο 14 παράγραφος 3 στοιχεία α) και β), η αναθέτουσα αρχή υποβάλλει έκθεση στην ομάδα συνεργασίας NIS, σε τακτική βάση και τουλάχιστον δύο φορές ετησίως, σχετικά με τη χρήση και τα αποτελέσματα της στήριξης.***

***12.*** ***Στην περίπτωση των χρηστών που αναφέρονται στο άρθρο 14 παράγραφος 3 στοιχείο γ), η Επιτροπή υποβάλλει έκθεση στο Συμβούλιο και ενημερώνει τον ύπατο εκπρόσωπο σε τακτική βάση και τουλάχιστον δύο φορές ετησίως σχετικά με τη χρήση και τα αποτελέσματα της στήριξης.***

# I

Άρθρο 17

Αξιόπιστοι πάροχοι διαχειριζόμενων υπηρεσιών ασφάλειας

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) 2024/2509 και σύμφωνα με τις ακόλουθες αρχές:

   α) διασφαλίζει ότι ***οι υπηρεσίες που περιλαμβάνονται στην*** εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας***, στο σύνολό τους, είναι τέτοιες ώστε η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας να*** περιλαμβάνει υπηρεσίες που μπορούν να αναπτυχθούν σε όλα τα κράτη μέλη, λαμβανομένων ιδίως υπόψη των εθνικών απαιτήσεων για την παροχή των εν λόγω υπηρεσιών, ***μεταξύ άλλων όσον αφορά τις γλώσσες, την πιστοποίηση ή τη διαπίστευση·***

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

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

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 και απαιτήσεις:

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 και συνέχεια της εμπειρογνωσίας, καθώς και τους απαιτούμενους τεχνικούς πόρους·

β) ***ο πάροχος και οποιεσδήποτε σχετικές θυγατρικές και υπεργολάβοι συμμορφώνονται με τους ισχύοντες κανόνες για την προστασία των διαβαθμισμένων πληροφοριών και εφαρμόζουν κατάλληλα μέτρα, συμπεριλαμβανομένων, κατά περίπτωση, συμφωνιών μεταξύ τους, για την προστασία των εμπιστευτικών πληροφοριών που αφορούν την υπηρεσία, και ιδίως των αποδεικτικών στοιχείων, των πορισμάτων και των εκθέσεων·***

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, ***όταν αυτό απαιτείται από ένα κράτος μέλος·***

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

στ) ***ο πάροχος διαθέτει το υλισμικό και το λογισμικό που απαιτούνται για τη στήριξη της ζητούμενης υπηρεσίας, τα οποία δεν περιέχουν γνωστές εκμεταλλεύσιμες ευπάθειες, περιλαμβάνουν τις τελευταίες ενημερώσεις ασφαλείας και, σε κάθε περίπτωση, συμμορφώνονται με οποιαδήποτε εφαρμοστέα διάταξη του κανονισμού (ΕΕ) 2024/... του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου***[23] [+]·

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 ***υψηλής κρισιμότητας ή οντότητες που δραστηριοποιούνται σε άλλους κρίσιμους τομείς·***

---

[23] ***Κανονισμός (ΕΕ) 2024/... του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της ..., σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία και για την τροποποίηση των κανονισμών (ΕΕ) αριθ. 168/2013 και (ΕΕ) 2019/1020 και της οδηγίας (ΕΕ) 2020/1828 (κανονισμός για την κυβερνοανθεκτικότητα) (ΕΕ L, …, ELI: …).***

[+] ***ΕΕ: Να προστεθεί στο κείμενο ο αριθμός του κανονισμού που περιέχει το έγγραφο PE-CONS 100/23 (2022/0272(COD)) και να προστεθεί ο αριθμός, η ημερομηνία, τα στοιχεία ΕΕ και τα στοιχεία ELI του εν λόγω κανονισμού στην υποσημείωση.***

η) ο πάροχος είναι σε θέση να παρέχει την υπηρεσία εντός σύντομου χρονικού διαστήματος στα κράτη μέλη όπου μπορεί να παρέχει την υπηρεσία·

θ) ***ο πάροχος είναι σε θέση να παρέχει την υπηρεσία σε μία ή περισσότερες επίσημες γλώσσες των θεσμικών οργάνων της Ένωσης ή κράτους μέλους, σύμφωνα με τις απαιτήσεις, εάν υπάρχουν, των κρατών μελών ή των χρηστών που αναφέρονται στο άρθρο 14 παράγραφος 3 στοιχεία β) και γ), στα οποία ή τους οποίους μπορεί ο πάροχος να παρέχει την υπηρεσία·***

ι) ***όταν τεθεί σε εφαρμογή ένα ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας για διαχειριζόμενες υπηρεσίες ασφάλειας σύμφωνα με τον κανονισμό (ΕΕ) 2019/881, ο πάροχος πιστοποιείται σύμφωνα με το εν λόγω σύστημα, εντός διαστήματος δύο ετών από την ημερομηνία εφαρμογής του συστήματος·***

***ια) ο πάροχος περιλαμβάνει στην προσφορά τους όρους μετατροπής για κάθε αχρησιμοποίητη υπηρεσία αντιμετώπισης περιστατικών που θα μπορούσε να μετατραπεί σε υπηρεσία ετοιμότητας που συνδέεται στενά με την αντιμετώπιση περιστατικών, όπως ασκήσεις ή προγράμματα κατάρτισης.***

***3. Για τους σκοπούς της προμήθειας υπηρεσιών για την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, η αναθέτουσα αρχή μπορεί, κατά περίπτωση, να αναπτύξει κριτήρια και απαιτήσεις επιπλέον εκείνων που αναφέρονται στην παράγραφο 2, σε στενή συνεργασία με τα κράτη μέλη.***

*Άρθρο 18*

*Αμοιβαία συνδρομή*

***1.*** ***Ο μηχανισμός έκτακτης ανάγκης για την κυβερνοασφάλεια παρέχει στήριξη για τεχνική συνδρομή που παρέχεται από ένα κράτος μέλος σε άλλο κράτος μέλος που επηρεάζεται από σημαντικό περιστατικό κυβερνοασφάλειας ή περιστατικό κυβερνοασφάλειας μεγάλης κλίμακας, μεταξύ άλλων στις περιπτώσεις που αναφέρονται στο άρθρο 11 παράγραφος 3 στοιχείο στ) της οδηγίας (ΕΕ) 2022/2555.***

***2.*** ***Η στήριξη για την τεχνική αμοιβαία συνδρομή που αναφέρεται στην παράγραφο 1 του παρόντος άρθρου παρέχεται με τη μορφή επιχορηγήσεων και υπό τους όρους που καθορίζονται στα σχετικά προγράμματα εργασίας όπως αναφέρονται στο άρθρο 24 του κανονισμού (ΕΕ) 2021/694.***

Άρθρο 19

Στήριξη σε τρίτες χώρες ***συνδεδεμένες με το*** πρόγραμμα «Ψηφιακή Ευρώπη»

1. ***Μια τρίτη χώρα συνδεδεμένη με το*** πρόγραμμα «Ψηφιακή Ευρώπη» ***μπορεί να ζητήσει στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, όταν η συμφωνία, μέσω της οποίας συνδέεται με το πρόγραμμα «Ψηφιακή Ευρώπη», προβλέπει συμμετοχή στην εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας. Η εν λόγω συμφωνία περιλαμβάνει διατάξεις που απαιτούν από την οικεία τρίτη χώρα συνδεδεμένη με το*** πρόγραμμα «Ψηφιακή Ευρώπη» ***να συμμορφώνεται με τις υποχρεώσεις που ορίζονται στις παραγράφους 2 και 9 του παρόντος άρθρου. Για τους σκοπούς της συμμετοχής τρίτης χώρας στην εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, η μερική σύνδεση τρίτης χώρας με το πρόγραμμα «Ψηφιακή Ευρώπη» μπορεί να περιλαμβάνει σύνδεση που περιορίζεται στον επιχειρησιακό στόχο που αναφέρεται στο άρθρο 6 παράγραφος στοιχείο ζ) του κανονισμού (ΕΕ) 2021/694.***

2. ***Εντός τριών μηνών από τη σύναψη της συμφωνίας που αναφέρεται στην παράγραφο 1 και σε κάθε περίπτωση*** πριν λάβουν στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, οι τρίτες χώρες ***συνδεδεμένες με το*** πρόγραμμα «Ψηφιακή Ευρώπη» παρέχουν στην Επιτροπή ▌ 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 ***περιστατικά κυβερνοασφάλειας, περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας, και περιστατικά ισοδύναμα με περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας***, καθώς και πληροφοριών σχετικά με τις αρμόδιες εθνικές οντότητες, συμπεριλαμβανομένων των ομάδων αντιμετώπισης περιστατικών ασφαλείας σε υπολογιστές ή ισοδύναμων οντοτήτων, τις ικανότητές τους και τους πόρους που τους διατίθενται. ***Η τρίτη χώρα συνδεδεμένη με το*** πρόγραμμα «Ψηφιακή Ευρώπη» ***παρέχει επικαιροποιήσεις των εν λόγω πληροφοριών σε τακτική βάση και τουλάχιστον μία φορά ετησίως. Η Επιτροπή κοινοποιεί τις πληροφορίες αυτές στον ύπατο εκπρόσωπο και τον ENISA με σκοπό να διευκολυνθεί η εφαρμογή που αναφέρεται στην παράγραφο 11.***

*3. Η Επιτροπή αξιολογεί τακτικά, και τουλάχιστον μία φορά ετησίως, τα ακόλουθα κριτήρια για κάθε τρίτη χώρα συνδεδεμένη με το* πρόγραμμα «Ψηφιακή Ευρώπη» *που αναφέρεται στην παράγραφο 1:*

*α) κατά πόσον η εν λόγω χώρα συμμορφώνεται με τους όρους της συμφωνίας που αναφέρεται στην παράγραφο 1, στον βαθμό που οι εν λόγω όροι σχετίζονται με τη συμμετοχή στην εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας·*

*β) κατά πόσον η εν λόγω χώρα έχει λάβει επαρκή μέτρα για την προετοιμασία για σημαντικά περιστατικά κυβερνοασφάλειας ή περιστατικά ισοδύναμα με περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας, με βάση τις πληροφορίες που αναφέρονται στην παράγραφο 2· και*

*γ) κατά πόσον η παροχή στήριξης συνάδει με την πολιτική της Ένωσης και τις συνολικές σχέσεις της με την εν λόγω χώρα, και κατά πόσον συνάδει με άλλες πολιτικές της Ένωσης στον τομέα της ασφάλειας.*

*Η Επιτροπή διαβουλεύεται με τον ύπατο εκπρόσωπο κατά τη διενέργεια της αξιολόγησης που αναφέρεται στο πρώτο εδάφιο, όσον αφορά το κριτήριο που αναφέρεται στο στοιχείο γ) του εν λόγω εδαφίου.*

*Εάν η Επιτροπή καταλήξει στο συμπέρασμα ότι μια τρίτη χώρα συνδεδεμένη με το πρόγραμμα «Ψηφιακή Ευρώπη» πληροί όλες τις προϋποθέσεις που αναφέρονται στο πρώτο εδάφιο, υποβάλλει πρόταση στο Συμβούλιο για την έκδοση εκτελεστικής πράξης σύμφωνα με την παράγραφο 4, με την οποία εγκρίνεται η παροχή στήριξης από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας στην εν λόγω χώρα.*

*4. Το Συμβούλιο μπορεί να εκδίδει τις εκτελεστικές πράξεις που αναφέρονται στην παράγραφο 3. Οι εν λόγω εκτελεστικές πράξεις έχουν μέγιστη ισχύ ενός έτους. Οι πράξεις αυτές μπορούν να ανανεώνονται. Μπορούν να περιλαμβάνουν όριο, το οποίο δεν μπορεί να είναι μικρότερο των 75 ημερών, όσον αφορά τον αριθμό των ημερών για τις οποίες μπορεί να παρασχεθεί στήριξη κατόπιν ενός μόνο αιτήματος.*

*Για τους σκοπούς του παρόντος άρθρου, το Συμβούλιο ενεργεί ταχέως και, κατά κανόνα, εκδίδει τις εκτελεστικές πράξεις που αναφέρονται στην παρούσα παράγραφο εντός οκτώ εβδομάδων από την έγκριση της οικείας πρότασης της Επιτροπής δυνάμει της παραγράφου 3 τρίτο εδάφιο.*

*5. Το Συμβούλιο μπορεί ανά πάσα στιγμή να τροποποιήσει ή να καταργήσει τις εκτελεστικές πράξεις που εκδίδονται δυνάμει της παραγράφου 4, κατόπιν πρότασης της Επιτροπής.*

*Εάν το Συμβούλιο κρίνει ότι έχει επέλθει σημαντική αλλαγή όσον αφορά το κριτήριο που αναφέρεται στην παράγραφο 3 πρώτο εδάφιο στοιχείο γ), το Συμβούλιο μπορεί να τροποποιήσει ή να καταργήσει εκτελεστική πράξη που έχει εκδοθεί δυνάμει της παραγράφου 4 ενεργώντας κατόπιν δεόντως αιτιολογημένης πρωτοβουλίας ενός ή περισσότερων κρατών μελών.*

*6. Κατά την άσκηση των εκτελεστικών αρμοδιοτήτων του δυνάμει του παρόντος άρθρου, το Συμβούλιο εφαρμόζει τα κριτήρια που αναφέρονται στην παράγραφο 3 πρώτο εδάφιο και εξηγεί την αξιολόγησή του όσον αφορά τα εν λόγω κριτήρια. Ειδικότερα, όταν ενεργεί με δική του πρωτοβουλία σύμφωνα με την παράγραφο 5 δεύτερο εδάφιο, το Συμβούλιο εξηγεί τη σημαντική αλλαγή που αναφέρεται στο εν λόγω εδάφιο.*

7. Η στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας ***προς τρίτη χώρα συνδεδεμένη με το*** πρόγραμμα «Ψηφιακή Ευρώπη» συμμορφώνεται με τυχόν ειδικούς όρους που καθορίζονται ***στη συμφωνία, όπως αναφέρεται*** στην παράγραφο 1.

8. Στους χρήστες από τρίτες χώρες συνδεδεμένες ***με το*** πρόγραμμα «Ψηφιακή Ευρώπη» που είναι επιλέξιμοι να λαμβάνουν υπηρεσίες από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας περιλαμβάνονται αρμόδιες αρχές, όπως ***ομάδες αντιμετώπισης περιστατικών ασφάλειας υπολογιστών*** ή ισοδύναμες οντότητες και αρχές διαχείρισης κυβερνοκρίσεων.

9. Κάθε τρίτη χώρα ***συνδεδεμένη με το*** πρόγραμμα «Ψηφιακή Ευρώπη» 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.

***10.*** ***Τα αιτήματα για στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας που υποβάλλονται δυνάμει του παρόντος άρθρου, αξιολογούνται από την Επιτροπή. Η αναθέτουσα αρχή μπορεί να παρέχει στήριξη σε τρίτη χώρα μόνον όταν, και για όσο χρονικό διάστημα, έχει τεθεί σε ισχύ εκτελεστική πράξη του Συμβουλίου που επιτρέπει τη στήριξη αυτή όσον αφορά την εν λόγω χώρα και που εκδίδεται δυνάμει της παραγράφου 4 του παρόντος άρθρου. Η απάντηση διαβιβάζεται στους χρήστες που αναφέρονται στο άρθρο 14 παράγραφος 3 στοιχείο γ) χωρίς αδικαιολόγητη καθυστέρηση.***

***11.*** ***Μόλις λάβει αίτημα στήριξης δυνάμει του παρόντος άρθρου, η Επιτροπή ενημερώνει αμέσως το Συμβούλιο. Η Επιτροπή τηρεί ενήμερο το Συμβούλιο σχετικά με την αξιολόγηση του αιτήματος.*** Η Επιτροπή ***συνεργάζεται επίσης*** με τον ύπατο εκπρόσωπο όσον αφορά τα αιτήματα που λαμβάνει και την υλοποίηση της στήριξης που παρέχεται σε τρίτες χώρες ***συνδεδεμένες με το*** πρόγραμμα «Ψηφιακή Ευρώπη» τρίτες χώρες από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας. ***Επιπλέον, η Επιτροπή θα πρέπει επίσης να λαμβάνει υπόψη τυχόν απόψεις που παρέχει ο ENISA σχετικά με τα αιτήματα αυτά.***

*Άρθρο 20*

*Συντονισμός με ενωσιακούς μηχανισμούς διαχείρισης κρίσεων*

***1.*** ***Σε περίπτωση που ένα σημαντικό περιστατικό κυβερνοασφάλειας, περιστατικό κυβερνοασφάλειας μεγάλης κλίμακας, ή περιστατικό ισοδύναμο με περιστατικό κυβερνοασφάλειας μεγάλης κλίμακας οφείλεται ή οδηγεί σε καταστροφή, όπως ορίζεται στο άρθρο 4 σημείο 1) της απόφασης αριθ. 1313/2013/ΕΕ, η στήριξη που παρέχεται βάσει του παρόντος κανονισμού για την αντιμετώπιση τέτοιου περιστατικού συμπληρώνει τις δράσεις δυνάμει και με την επιφύλαξη της εν λόγω απόφασης.***

***2.*** ***Σε περίπτωση περιστατικού κυβερνοασφάλειας μεγάλης κλίμακας ή περιστατικού ισοδύναμου με περιστατικό κυβερνοασφάλειας μεγάλης κλίμακας, όπου ενεργοποιούνται οι ρυθμίσεις για την ολοκληρωμένη αντιμετώπιση πολιτικών κρίσεων της ΕΕ δυνάμει της εκτελεστικής απόφασης (ΕΕ) 2018/1993 (ρυθμίσεις IPCR), η στήριξη που παρέχεται βάσει του παρόντος κανονισμού για την αντιμετώπιση του εν λόγω περιστατικού αντιμετωπίζεται σύμφωνα με τις σχετικές διαδικασίες στο πλαίσιο των ρυθμίσεων IPCR.***

Κεφάλαιο IV

ΕΥΡΩΠΑΪΚΟΣ ΜΗΧΑΝΙΣΜΟΣ ΕΞΕΤΑΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Άρθρο 21

Ευρωπαϊκός μηχανισμός εξέτασης περιστατικών κυβερνοασφάλειας

1. Κατόπιν αιτήματος της Επιτροπής ***ή του EU-CyCLONe, ο ENISA, με την υποστήριξη του δικτύου CSIRT και με την έγκριση του οικείου κράτους μέλους, εξετάζει και αξιολογεί κυβερνοαπειλές, γνωστές εκμεταλλεύσιμες*** ευπάθειες και δράσεις μετριασμού σε σχέση με συγκεκριμένο σημαντικό ***περιστατικό κυβερνοασφάλειας*** ή ***περιστατικό κυβερνοασφάλειας*** μεγάλης κλίμακας. Μετά την ολοκλήρωση της εξέτασης και της αξιολόγησης ενός περιστατικού και ***με στόχο την άντληση διδαγμάτων για την αποφυγή ή τον μετριασμό μελλοντικών περιστατικών***, ο ENISA υποβάλλει έκθεση εξέτασης περιστατικού ***στο EU-CyCLONe,*** στο δίκτυο CSIRT, ***στο οικείο κράτος μέλος*** 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. ***Όταν ένα συμβάν έχει αντίκτυπο σε τρίτη χώρα συνδεδεμένη με το*** πρόγραμμα «Ψηφιακή Ευρώπη»***, ο ENISA κοινοποιεί την έκθεση στο Συμβούλιο. Σε τέτοιες περιπτώσεις***, η Επιτροπή κοινοποιεί την έκθεση στον Ύπατο Εκπρόσωπο.

2. Για την εκπόνηση της έκθεσης εξέτασης περιστατικού που αναφέρεται στην παράγραφο 1 του παρόντος άρθρου, ο ENISA συνεργάζεται με όλα τα σχετικά ενδιαφερόμενα μέρη ***και συγκεντρώνει τις παρατηρήσεις τους***, συμπεριλαμβανομένων εκπροσώπων των κρατών μελών, της Επιτροπής, άλλων σχετικών θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης, ***καθώς και εκπροσώπων του κλάδου, συμπεριλαμβανομένων των*** παρόχων διαχειριζόμενων υπηρεσιών ασφάλειας και ***των*** χρηστών υπηρεσιών κυβερνοασφάλειας. Κατά περίπτωση, ο ENISA***, σε συνεργασία με τις CSIRT και, όπου ενδείκνυται, τις αρμόδιες αρχές που έχουν οριστεί ή έχουν θεσπιστεί δυνάμει του άρθρου 8 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555, συνεργάζεται επίσης με οντότητες που επηρεάζονται από σημαντικά περιστατικά κυβερνοασφάλειας ή περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας***. Οι εκπρόσωποι των οποίων ζητείται η γνώμη γνωστοποιούν κάθε πιθανή σύγκρουση συμφερόντων.

3. Η αρχική έκθεση εξέτασης που αναφέρεται στην παράγραφο 1 του παρόντος άρθρου καλύπτει εξέταση και ανάλυση του συγκεκριμένου σημαντικού περιστατικού κυβερνοασφάλειας ή περιστατικού κυβερνοασφάλειας μεγάλης κλίμακας, συμπεριλαμβανομένων των κύριων αιτίων, των ***γνωστών εκμεταλλεύσιμων*** ευπαθειών και των διδαγμάτων που αντλήθηκαν. ***Ο ENISA διασφαλίζει ότι η έκθεση συμμορφώνεται*** με το ενωσιακό ή το εθνικό δίκαιο σχετικά με την προστασία ευαίσθητων ή διαβαθμισμένων πληροφοριών. ***Εάν το ζητήσουν τα οικεία κράτη μέλη ή άλλοι χρήστες που αναφέρονται στο άρθρο 14 παράγραφος 3 που επηρεάζονται από το περιστατικό, τα δεδομένα και οι πληροφορίες που περιέχονται στην έκθεση ανωνυμοποιούνται. Δεν περιλαμβάνει λεπτομέρειες σχετικά με ευπάθειες που αποτελούν αντικείμενο ενεργού εκμετάλλευσης και δεν έχουν ακόμα αρθεί.***

4. Κατά περίπτωση, η έκθεση εξέτασης περιστατικού διατυπώνει συστάσεις για τη βελτίωση της κατάστασης κυβερνοασφάλειας της Ένωσης ***και μπορεί να περιλαμβάνει βέλτιστες πρακτικές και διδάγματα που αντλήθηκαν από τα σχετικά ενδιαφερόμενα μέρη***.

5. ***Ο ENISA μπορεί να εκδώσει δημόσια διαθέσιμη έκδοση της έκθεσης εξέτασης περιστατικού. Η εν λόγω έκδοση της έκθεσης περιλαμβάνει μόνο αξιόπιστες δημόσιες πληροφορίες, ή άλλες αξιόπιστες πληροφορίες με τη συγκατάθεση των οικείων κρατών μελών και, όσον αφορά τις πληροφορίες σε σχέση με χρήστη όπως αναφέρεται στο άρθρο 14 παράγραφος 3 στοιχείο β) ή γ), με τη συγκατάθεση του εν λόγω χρήστη.***

Κεφάλαιο V

ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 22

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) παρεμβάλλεται το ακόλουθο στοιχείο:

«αα) στήριξη της ανάπτυξης ***ευρωπαϊκού συστήματος προειδοποίησης για την κυβερνοασφάλεια που θεσπίζεται με το άρθρο 3 του κανονισμού (ΕΕ) 2024/… του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου**** [+] ***(κανονισμός για την αλληλεγγύη στον κυβερνοχώρο),*** συμπεριλαμβανομένων της ανάπτυξης, της εγκατάστασης και της λειτουργίας εθνικών ***κυβερνοκόμβων και διασυνοριακών κυβερνοκόμβων*** που συμβάλλουν στην αντίληψη της κατάστασης στην Ένωση και στην ενίσχυση των ικανοτήτων της Ένωσης όσον αφορά τη συλλογή πληροφοριών για κυβερνοαπειλές·

---

* ***Κανονισμός (ΕΕ) 2024/… του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της …, σχετικά με τον καθορισμό μέτρων για την ενίσχυση της αλληλεγγύης και των ικανοτήτων της Ένωσης για την ανίχνευση, την προετοιμασία και την αντιμετώπιση κυβερνοαπειλών και περιστατικών κυβερνοασφάλειας και για την τροποποίηση του κανονισμού (ΕΕ) 2021/694 (κανονισμός για την αλληλεγγύη στον κυβερνοχώρο)… (ΕΕ L, …, ELI: …).».***

---

[+] ***ΕΕ: Να προστεθεί στο κείμενο ο αριθμός του κανονισμού που περιέχεται στο έγγραφο PE-CONS 94/24 (2023/0109(COD)) και να προστεθεί ο αριθμός, η ημερομηνία, η παραπομπή στην ΕΕ και η παραπομπή ELI του εν λόγω κανονισμού στην υποσημείωση.***

ii) προστίθεται το ακόλουθο στοιχείο:

«ζ) σύσταση και λειτουργία μηχανισμού έκτακτης ανάγκης ***για την κυβερνοασφάλεια*** που θεσπίζεται με το άρθρο 10 του κανονισμού (ΕΕ) 2024/…[24+]**,** συμπεριλαμβανομένης της δημιουργίας εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας ***η οποία θεσπίζεται με το άρθρο 14 του εν λόγω κανονισμού***, για τη στήριξη των κρατών μελών κατά την προετοιμασία και την αντιμετώπιση σημαντικών περιστατικών κυβερνοασφάλειας και περιστατικών κυβερνοασφάλειας υψηλής κλίμακας, συμπληρωματικά προς τους εθνικούς πόρους και ικανότητες και άλλες μορφές στήριξης που διατίθενται σε επίπεδο Ένωσης, και την στήριξη άλλων χρηστών στην αντιμετώπιση σημαντικών περιστατικών κυβερνοασφάλειας ή περιστατικών ***ισοδύναμων με περιστατικά*** κυβερνοασφάλειας μεγάλης κλίμακας·»·

β) η παράγραφος 2 αντικαθίσταται από το ακόλουθο κείμενο:

«2. ***Οι δράσεις στο πλαίσιο του ειδικού στόχου 3 εκτελούνται πρωτίστως μέσω του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας και του δικτύου εθνικών κέντρων συντονισμού, σύμφωνα με τον κανονισμό (ΕΕ) 2021/887 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου*. Ωστόσο η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας υλοποιείται από την Επιτροπή και, σύμφωνα με το άρθρο 14 παράγραφος 6 του κανονισμού (ΕΕ) 2024/...[+], 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).».***

---

[+] ***ΕΕ: Να προστεθεί στο κείμενο ο αριθμός του κανονισμού που περιέχεται στο έγγραφο PE-CONS 94/24 (2023/0109(COD)).***

2) Το άρθρο 9 τροποποιείται ως εξής:

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

«β) ***1 760 806 000*** EUR για τον ειδικό στόχο 2 – «Τεχνητή νοημοσύνη»,

γ) ***1 372 020 000*** EUR για τον ειδικό στόχο 3 – «Κυβερνοασφάλεια και εμπιστοσύνη»,

δ) ***482 640 000*** EUR για τον ειδικό στόχο 4 – «Προηγμένες ψηφιακές δεξιότητες,»·

β) προστίθεται η ακόλουθη παράγραφος 8:

«8. ***Κατά παρέκκλιση από το άρθρο 12 παράγραφος 1*** του δημοσιονομικού κανονισμού, οι μη χρησιμοποιηθείσες πιστώσεις αναλήψεων υποχρεώσεων και πληρωμών για δράσεις ***στο πλαίσιο της εφαρμογής της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας και για τις δράσεις στήριξης της αμοιβαίας συνδρομής δυνάμει του κανονισμού (ΕΕ) 2024/…[+],*** 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. ***Το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο ενημερώνονται σχετικά με τις πιστώσεις που μεταφέρονται σύμφωνα με το άρθρο 12 παράγραφος 6 του δημοσιονομικού κανονισμού.***».

[+] ***ΕΕ: Να προστεθεί στο κείμενο ο αριθμός του κανονισμού που περιέχεται στο έγγραφο PE-CONS 94/24 (2023/0109(COD)).***

*3) Το άρθρο 12 τροποποιείται ως εξής:*

*α) παρεμβάλλονται οι ακόλουθες παράγραφοι:*

*«5α. Η παράγραφος 5 δεν εφαρμόζεται, όσον αφορά νομικές οντότητες που είναι εγκατεστημένες στην Ένωση αλλά ελέγχονται από τρίτες χώρες, σε οποιαδήποτε δράση υλοποίησης του ευρωπαϊκού συστήματος προειδοποίησης για την κυβερνοασφάλεια, εφόσον πληρούνται αμφότερες οι ακόλουθες προϋποθέσεις όσον αφορά την εν λόγω δράση:*

*α) υπάρχει πραγματικός κίνδυνος, λαμβανομένων υπόψη των αποτελεσμάτων της χαρτογράφησης που διενεργείται δυνάμει του άρθρου 9 παράγραφος 4 του κανονισμού (ΕΕ) 2024/...[+], τα εργαλεία, οι υποδομές ή οι υπηρεσίες που είναι αναγκαία και επαρκή για την εν λόγω δράση ώστε αυτή να συμβάλει επαρκώς στην επίτευξη του στόχου του ευρωπαϊκού συστήματος προειδοποίησης για την κυβερνοασφάλεια, να μη διατίθενται από νομικές οντότητες που είναι ή θεωρούνται εγκατεστημένες σε κράτη μέλη και ελέγχονται από κράτη μέλη ή από υπηκόους κρατών μελών·*

*β) ο κίνδυνος ασφαλείας που συνεπάγεται η προμήθεια από τις εν λόγω νομικές οντότητες στο πλαίσιο του ευρωπαϊκού συστήματος προειδοποίησης για την κυβερνοασφάλεια είναι ανάλογος προς τα οφέλη και δεν υπονομεύει τα ουσιώδη συμφέροντα ασφάλειας της Ένωσης και των κρατών μελών της.*

[+] *ΕΕ: να προστεθεί στο κείμενο ο αριθμός του κανονισμού που περιέχει το έγγραφο PE-CONS 94/24 (2023/0109(COD)).*

***5β. Η παράγραφος 5 δεν εφαρμόζεται, όσον αφορά νομικές οντότητες που είναι εγκατεστημένες στην Ένωση αλλά ελέγχονται από τρίτες χώρες, σε δράσεις υλοποίησης της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, εφόσον πληρούνται αμφότερες οι ακόλουθες προϋποθέσεις όσον αφορά την εν λόγω δράση:***

***α) υπάρχει πραγματικός κίνδυνος, λαμβανομένων υπόψη των αποτελεσμάτων της χαρτογράφησης που διενεργείται δυνάμει του άρθρου 14 παράγραφος 6 του κανονισμού (ΕΕ) 2024./...[+], η τεχνολογία, η εμπειρογνωσία ή ικανότητα που είναι αναγκαίες και επαρκείς για την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας ώστε αυτή να εκτελεί επαρκώς τις λειτουργίες της, να μη διατίθενται από νομικές οντότητες που είναι ή θεωρούνται εγκατεστημένες σε κράτη μέλη και ελέγχονται από κράτη μέλη ή από υπηκόους κρατών μελών·***

***β) ο κίνδυνος ασφαλείας που συνεπάγεται η συμπερίληψη των εν λόγω νομικών οντοτήτων στην εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας είναι ανάλογος προς τα οφέλη και δεν υπονομεύει τα ουσιώδη συμφέροντα ασφάλειας της Ένωσης και των κρατών μελών της.»·***

*β) η παράγραφος 6 αντικαθίσταται από το ακόλουθο κείμενο:*

*«6. Για δεόντως αιτιολογημένους λόγους ασφάλειας, το πρόγραμμα εργασίας μπορεί επίσης να προβλέπει ότι νομικές οντότητες που είναι εγκατεστημένες σε συνδεδεμένες χώρες και οι νομικές οντότητες που είναι εγκατεστημένες στην Ένωση αλλά ελέγχονται από τρίτες χώρες μπορούν να είναι επιλέξιμες για συμμετοχή σε όλες ή σε ορισμένες δράσεις στο πλαίσιο των ειδικών στόχων 1 και 2, μόνο εάν τηρούν τις απαιτήσεις τις οποίες πρέπει να πληρούν οι εν λόγω νομικές οντότητες, ώστε να κατοχυρώνεται η προστασία των ουσιωδών συμφερόντων ασφάλειας της Ένωσης και των κρατών μελών και να εξασφαλίζεται η προστασία των πληροφοριών που περιέχονται σε διαβαθμισμένα έγγραφα. Οι εν λόγω απαιτήσεις ορίζονται στο πρόγραμμα εργασίας.*

***Το πρώτο εδάφιο εφαρμόζεται επίσης, όσον αφορά νομικές οντότητες που είναι εγκατεστημένες στην Ένωση αλλά ελέγχονται από τρίτες χώρες, σε δράσεις στο πλαίσιο του ειδικού στόχου 3:***

***α) για την εφαρμογή του ευρωπαϊκού συστήματος προειδοποίησης για την κυβερνοασφάλεια σε περιπτώσεις όπου εφαρμόζεται η παράγραφος 5α· και***

***β) για την υλοποίηση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας σε περιπτώσεις όπου εφαρμόζεται η παράγραφος 5β.».***

4) Στο άρθρο 14, η παράγραφος 2 αντικαθίσταται από το ακόλουθο κείμενο:

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

Αν η επίτευξη του στόχου μίας δράσης απαιτεί την προμήθεια καινοτόμων αγαθών και υπηρεσιών, οι επιχορηγήσεις μπορούν να παρασχεθούν μόνο σε δικαιούχους που είναι αναθέτουσες αρχές ή αναθέτοντες φορείς όπως ορίζονται στις οδηγίες 2014/24/ΕΕ* και 2014/25/ΕΕ** 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, 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 του παρόντος κανονισμού. Η Επιτροπή και ο ENISA μπορούν επίσης να ενεργούν ως χονδρέμποροι, αγοράζοντας, αποθηκεύοντας και μεταπωλώντας ή δωρίζοντας προμήθειες και υπηρεσίες, συμπεριλαμβανομένων των ενοικίων, στις εν λόγω τρίτες χώρες. Κατά παρέκκλιση από το άρθρο 168 παράγραφος 3 του κανονισμού (ΕΕ, Ευρατόμ) ***2024/2509 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου****, το αίτημα από μία μόνο τρίτη χώρα 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, η Επιτροπή και ο ENISA μπορούν να ενεργούν ως κεντρική αρχή προμηθειών για την προμήθεια για λογαριασμό ή εξ ονόματος των θεσμικών και λοιπών οργάνων ή 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 ή οργανισμούς της Ένωσης. Κατά παρέκκλιση από το άρθρο 168 παράγραφος 3 του κανονισμού (ΕΕ, Ευρατόμ) ***2024/2509***[+], 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 μέσων στο πλαίσιο συνδυαστικών πράξεων.

---

* Οδηγία 2014/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Φεβρουαρίου 2014, σχετικά με τις δημόσιες προμήθειες και την κατάργηση της οδηγίας 2004/18/ΕΚ (ΕΕ L 94 της 28.3.2014, σ. 65).

** Οδηγία 2014/25/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ηςΦεβρουαρίου 2014, σχετικά με τις προμήθειες φορέων που δραστηριοποιούνται στους τομείς του ύδατος, της ενέργειας, των μεταφορών και των ταχυδρομικών υπηρεσιών και την κατάργηση της οδηγίας 2004/17/ΕΚ (ΕΕ L 94 της 28.3.2014, σ. 243).

*** ***Κανονισμός (ΕΕ, Ευρατόμ) 2024/2509 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Σεπτεμβρίου 2024, σχετικά με τους δημοσιονομικούς κανόνες που εφαρμόζονται στον γενικό προϋπολογισμό της Ένωσης (ΕΕ L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj)***.».

5) Παρεμβάλλεται το ακόλουθο άρθρο:

***«Άρθρο 16α***

***Σύγκρουση κανόνων***

Στην περίπτωση δράσεων που υλοποιούν ***το ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια***, οι εφαρμοστέοι κανόνες είναι εκείνοι που ορίζονται στα άρθρα 4, 5 και 9 του κανονισμού (ΕΕ) …/…[+]. Σε περίπτωση σύγκρουσης των διατάξεων του παρόντος κανονισμού με τα άρθρα 4, 5 και 9 του κανονισμού (ΕΕ) 2024/…[+], τα τελευταία υπερισχύουν και εφαρμόζονται επί των εν λόγω συγκεκριμένων δράσεων.

***Στην περίπτωση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, οι ειδικοί κανόνες για τη συμμετοχή τρίτων χωρών που συνδέονται με το πρόγραμμα καθορίζονται στο άρθρο 19 του κανονισμού (ΕΕ) 2024/…[+]. Σε περίπτωση σύγκρουσης των διατάξεων του παρόντος κανονισμού με το άρθρο 19 του κανονισμού (ΕΕ) 2024/…[+], το τελευταίο υπερισχύει και εφαρμόζεται επί των εν λόγω συγκεκριμένων δράσεων.».***

[+] ***ΕΕ: να προστεθεί στο κείμενο ο αριθμός του κανονισμού που περιέχει το έγγραφο PE-CONS 94/24 (2023/0109(COD))***

6) Το άρθρο 19 αντικαθίσταται από το ακόλουθο κείμενο:

«Άρθρο 19
Επιχορηγήσεις

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

Στήριξη με τη μορφή επιχορηγήσεων μπορεί να χορηγείται απευθείας από το ***ΕΚΑΚ*** χωρίς πρόσκληση υποβολής προτάσεων προς ***τα επιλεγμένα κράτη μέλη δυνάμει του*** άρθρου 9 του κανονισμού ***(ΕΕ) 2024/...***[+], και την κοινοπραξία υποδοχής που αναφέρεται στο άρθρο 5 του κανονισμού ***(ΕΕ) 2024/…***[+], σύμφωνα με το άρθρο 195 παράγραφος 1 στοιχείο δ) του ▌ δημοσιονομικού κανονισμού.

Στήριξη με τη μορφή επιχορηγήσεων για τον μηχανισμό έκτακτης ανάγκης ***για την κυβερνοασφάλεια*** μπορεί να χορηγείται απευθείας από το ***ΕΚΑΚ*** στα κράτη μέλη χωρίς πρόσκληση υποβολής προτάσεων, σύμφωνα με το άρθρο 195 παράγραφος 1 στοιχείο δ) ***του δημοσιονομικού κανονισμού***.

[+] ***ΕΕ: να προστεθεί στο κείμενο ο αριθμός του κανονισμού που περιέχει το έγγραφο PE-CONS 94/24 (2023/0109(COD)).***

Για τις δράσεις στήριξης της αμοιβαίας συνδρομής που προβλέπονται στο άρθρο 18 του κανονισμού ***(ΕΕ) 2024./...***[+], το ***ΕΚΑΚ*** ενημερώνει την Επιτροπή και τον ENISA σχετικά με τα αιτήματα των κρατών μελών για άμεσες επιχορηγήσεις χωρίς πρόσκληση υποβολής προτάσεων.

Για τις δράσεις στήριξης της αμοιβαίας συνδρομής που προβλέπονται στο άρθρο 18 του κανονισμού ***(ΕΕ) 2024/…***[+], και σύμφωνα με το άρθρο 193 παράγραφος 2 δεύτερο εδάφιο στοιχείο α) ***του δημοσιονομικού κανονισμού***, σε δεόντως αιτιολογημένες περιπτώσεις, οι δαπάνες μπορούν να θεωρηθούν επιλέξιμες ακόμη και αν πραγματοποιήθηκαν πριν από την υποβολή της αίτησης επιχορήγησης.***»***.

7) Τα παραρτήματα I και II τροποποιούνται σύμφωνα με το παράρτημα του παρόντος κανονισμού.

[+] ***ΕΕ: να προστεθεί στο κείμενο ο αριθμός του κανονισμού που περιέχει το έγγραφο PE-CONS 94/24 (2023/0109(COD)).***

*Άρθρο 23*

*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 14 παράγραφος 7 εξουσία έκδοσης κατ' εξουσιοδότηση πράξεων ανατίθεται στην Επιτροπή για χρονικό διάστημα πέντε ετών από την ... [ημερομηνία έναρξης ισχύος του παρόντος κανονισμού]. Η Επιτροπή υποβάλλει έκθεση σχετικά με τις εξουσίες που της έχουν ανατεθεί το αργότερο εννέα μήνες πριν από τη λήξη της περιόδου των πέντε 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 14 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. Η κατ' εξουσιοδότηση πράξη που εκδίδεται δυνάμει του άρθρου 14 παράγραφος 7 τίθεται σε ισχύ εφόσον δεν έχει διατυπωθεί αντίρρηση από το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο εντός δύο μηνών από την ημέρα που η πράξη κοινοποιείται στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο ή αν, πριν λήξει αυτή η περίοδος, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο ενημερώσουν αμφότερα την Επιτροπή ότι δεν θα προβάλουν αντιρρήσεις. Η προθεσμία αυτή παρατείνεται κατά δύο μήνες κατόπιν πρωτοβουλίας του Ευρωπαϊκού Κοινοβουλίου ή του Συμβουλίου.***

Άρθρο 24

Διαδικασία επιτροπής

1. Η Επιτροπή επικουρείται από την επιτροπή συντονισμού του προγράμματος «Ψηφιακή Ευρώπη» που αναφέρεται στο άρθρο 31 παράγραφος 1 του κανονισμού (ΕΕ) 2021/694. Η εν λόγω επιτροπή αποτελεί 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 25

Αξιολόγηση ***και επανεξέταση***

***1. Έως … [δύο έτη από την ημερομηνία εφαρμογής του παρόντος κανονισμού] και ακολούθως τουλάχιστον ανά τέσσερα έτη, η Επιτροπή αξιολογεί την λειτουργία των μέτρων που προβλέπονται στον παρόντα κανονισμό και υποβάλλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο.***

***2. Στο πλαίσιο της αξιολόγησης που αναφέρεται στην παράγραφο 1 αξιολογούνται ειδικότερα:***

***α) ο αριθμός των εθνικών κυβερνοκόμβων και των διασυνοριακών κυβερνοκόμβων που δημιουργήθηκαν, η έκταση των πληροφοριών που ανταλλάσσονται, συμπεριλαμβανομένων, εάν είναι δυνατόν, του αντικτύπου στο έργο του δικτύου CSIRT, και ο βαθμός στον οποίο οι εν λόγω κόμβοι έχουν συμβάλει στην ενίσχυση της κοινής ενωσιακής ανίχνευσης και αντίληψης της κατάστασης όσον αφορά κυβερνοαπειλές και περιστατικά, καθώς και στην ανάπτυξη τεχνολογιών αιχμής· και η χρήση της χρηματοδότησης του προγράμματος «Ψηφιακή Ευρώπη» για εργαλεία, υποδομές ή υπηρεσίες κυβερνοασφάλειας που αγοράζονται από κοινού, και, εάν οι πληροφορίες είναι διαθέσιμες, το επίπεδο συνεργασίας μεταξύ των εθνικών κυβερνοκόμβων και των τομεακών και διατομεακών κοινοτήτων βασικών και σημαντικών οντοτήτων όπως αναφέρεται στο άρθρο 3 της οδηγίας (ΕΕ) 2022/2555·***

*β) η χρήση και η αποτελεσματικότητα των δράσεων στο πλαίσιο του μηχανισμού έκτακτης ανάγκης για την κυβερνοασφάλεια που στηρίζουν την ετοιμότητα, συμπεριλαμβανομένων προγραμμάτων κατάρτισης, αντιμετώπισης σημαντικών περιστατικών κυβερνοασφάλειας, περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας και περιστατικών ισοδύναμων με περιστατικά κυβερνοασφάλειας μεγάλης κλίμακας, και αρχικής ανάκαμψης από αυτά, καθώς και η χρήση της χρηματοδότησης του προγράμματος «Ψηφιακή Ευρώπη» και των διδαγμάτων και των συστάσεων που προκύπτουν από την εφαρμογή του μηχανισμού έκτακτης ανάγκης για την κυβερνοασφάλεια·*

*γ) η χρήση και η αποτελεσματικότητα της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας σε σχέση με τα είδη των χρηστών, συμπεριλαμβανομένης της χρήσης της χρηματοδότησης του προγράμματος «Ψηφιακή Ευρώπη», η υιοθέτηση υπηρεσιών, συμπεριλαμβανομένου του είδους τους, ο μέσος χρόνος ανταπόκρισης στα αιτήματα και ανάπτυξης της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, το ποσοστό των υπηρεσιών που μετατρέπονται σε υπηρεσίες ετοιμότητας που σχετίζονται με την πρόληψη και την αντιμετώπιση περιστατικών, καθώς και τα διδάγματα και οι συστάσεις που προκύπτουν από την υλοποίηση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας·*

*δ) η συμβολή του παρόντος κανονισμού στην ενίσχυση της ανταγωνιστικής θέσης της βιομηχανίας και των υπηρεσιών στην Ένωση, σε ολόκληρη την ψηφιακή οικονομία, συμπεριλαμβανομένων των πολύ μικρών και των μικρών και μεσαίων επιχειρήσεων, καθώς και των νεοφυών επιχειρήσεων, και η συμβολή στον γενικό στόχο της ενίσχυσης των δεξιοτήτων και ικανοτήτων κυβερνοασφάλειας του εργατικού δυναμικού.*

*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 26

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 Ι, το τμήμα «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 αντίληψη της κατάστασης στον κυβερνοχώρο συμπεριλαμβανομένων των εθνικών ***κυβερνοκόμβων*** και των διασυνοριακών ***κυβερνοκόμβων*** που απαρτίζουν ***το ευρωπαϊκό σύστημα προειδοποίησης για την κυβερνοασφάλεια***, 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 εκδίπλωσης αποτελεσματικών λύσεων αιχμής στους τομείς της κυβερνοασφάλειας και της εμπιστοσύνης σε όλα τα κράτη μέλη. Η εν λόγω εκδίπλωση 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 έλλειμμα δεξιοτήτων κυβερνοασφάλειας, ***λαμβανομένης υπόψη της ισόρροπης εκπροσώπησης των φύλων,*** για παράδειγμα, με την ευθυγράμμιση των προγραμμάτων για τις δεξιότητες κυβερνοασφάλειας, την προσαρμογή τους σε συγκεκριμένες τομεακές ανάγκες και τη διευκόλυνση της πρόσβασης σε στοχευμένη εξειδικευμένη κατάρτιση.

5. Προώθηση της αλληλεγγύης μεταξύ των κρατών μελών όσον αφορά την προετοιμασία και την αντιμετώπιση σημαντικών περιστατικών κυβερνοασφάλειας και περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας μέσω της ανάπτυξης υπηρεσιών κυβερνοασφάλειας σε διασυνοριακό επίπεδο, συμπεριλαμβανομένης της στήριξης για αμοιβαία συνδρομή μεταξύ των δημόσιων αρχών και της δημιουργίας εφεδρείας αξιόπιστων παρόχων διαχειριζόμενων υπηρεσιών ασφάλειας σε επίπεδο Ένωσης.»·

2) Στο παράρτημα ΙΙ, το τμήμα «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***, μεταξύ άλλων στο πλαίσιο του ευρωπαϊκού συστήματος προειδοποίησης για την κυβερνοασφάλεια***

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

3.3 Ο αριθμός των δράσεων που στηρίζουν την ετοιμότητα και την αντιμετώπιση περιστατικών κυβερνοασφάλειας στο πλαίσιο του μηχανισμού έκτακτης ανάγκης για την κυβερνοασφάλεια».

---

Έχει γίνει δήλωση σχετικά με τον παρόντα κανονισμό η οποία βρίσκεται στην … [ΕΕ: να σημειωθεί: ΕΕ C XXX της XX.XX.2024, σ. XX] και στον ακόλουθο σύνδεσμο: [ΕΕ: να εισαχθεί ο σύνδεσμος της δήλωσης].

***Δήλωση της Επιτροπής σχετικά με τον προϋπολογισμό όσον αφορά τον κανονισμό του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τον καθορισμό μέτρων για την ενίσχυση της αλληλεγγύης και των ικανοτήτων της Ένωσης για την ανίχνευση, την προετοιμασία και την αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας (Κανονισμός για την αλληλεγγύη στον κυβερνοχώρο)*** [*]

1. Το νομοθετικό δημοσιονομικό δελτίο της Επιτροπής που συνοδεύει την πρόταση κανονισμού για την αλληλεγγύη στον κυβερνοχώρο δημοσιεύθηκε τον Απρίλιο του 2023. Έκτοτε, τα σχετικά εκτιμώμενα ποσά έχουν αλλάξει λόγω της έκδοσης ή της αναμενόμενης έκδοσης άλλων νομοθετικών πράξεων.

2. Στις 5 Μαρτίου 2024, οι συννομοθέτες κατέληξαν σε προκαταρκτική πολιτική συμφωνία για τον περιορισμό σε 22 εκατ. EUR της ανακατανομής από τον ειδικό στόχο 4 «Προηγμένες ψηφιακές δεξιότητες» στον ειδικό στόχο 3 «Κυβερνοασφάλεια και εμπιστοσύνη» του προγράμματος «Ψηφιακή Ευρώπη» που προβλέπεται στο νομοθετικό δημοσιονομικό δελτίο.

3. Προκειμένου να αποτυπώνονται στο κείμενο οι όροι της προκαταρκτικής πολιτικής συμφωνίας, η Επιτροπή επικαιροποίησε το νομοθετικό δημοσιονομικό δελτίο του κανονισμού για την αλληλεγγύη στον κυβερνοχώρο όσον αφορά τα χρηματοδοτικά κονδύλια για τους ειδικούς στόχους 2 «Τεχνητή νοημοσύνη», 3 «Κυβερνοασφάλεια και εμπιστοσύνη» και 4 «Προηγμένες ψηφιακές δεξιότητες», λαμβάνοντας υπόψη τις ανακατανομές που συμφωνήθηκαν από τους συννομοθέτες.

4. Κατά συνέπεια, τα χρηματοδοτικά κονδύλια για την περίοδο 2025-2027 που παρουσιάζονται στο επικαιροποιημένο νομοθετικό δημοσιονομικό δελτίο, με την επιφύλαξη των εξουσιών της Επιτροπής στο πλαίσιο της ετήσιας διαδικασίας του προϋπολογισμού, είναι τα ακόλουθα:

   – [544 726 000 EUR] για τον ειδικό στόχο 2 «Τεχνητή νοημοσύνη», λαμβανομένου υπόψη ποσού 65 εκατ. EUR που ανακατανέμεται στον ειδικό στόχο 3 «Κυβερνοασφάλεια και εμπιστοσύνη»·

[*] Η προσωρινή πολιτική συμφωνία ορίζει εν κατακλείδι ότι η παρούσα δήλωση της Ευρωπαϊκής Επιτροπής θα δημοσιευθεί στη σειρά C της Επίσημης Εφημερίδας, και θα υπάρξει παραπομπή και σύνδεσμος προς αυτή στη σειρά L, μαζί με τη νομοθετική πράξη.

– [44 451 000 EUR] για τον ειδικό στόχο 3 «Κυβερνοασφάλεια και εμπιστοσύνη» – εν μέρει υπό την άμεση διαχείριση της Επιτροπής, συμπεριλαμβανομένου ποσού 26 εκατ. EUR που ανακατανέμεται από τους ειδικούς στόχους 2 και 4·

– [353 190 613 EUR] για τον ειδικό στόχο 3 «Κυβερνοασφάλεια και εμπιστοσύνη» – εν μέρει υπό τη διαχείριση του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας, συμπεριλαμβανομένου ποσού 61 εκατ. EUR που ανακατανέμεται από τους ειδικούς στόχους 2 και 4·

– [167 162 423 EUR] για τον ειδικό στόχο 4 «Προηγμένες ψηφιακές δεξιότητες», λαμβανομένου υπόψη ποσού 65 εκατ. EUR που ανακατανέμεται στον ειδικό στόχο 3 «Κυβερνοασφάλεια και εμπιστοσύνη».

5. Η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας θα χρηματοδοτηθεί από το χρηματοδοτικό κονδύλιο του ειδικού στόχου 3 «Κυβερνοασφάλεια και εμπιστοσύνη» – εν μέρει υπό την άμεση διαχείριση της Επιτροπής (το εν λόγω μέρος, σύμφωνα με το επικαιροποιημένο νομοθετικό δημοσιονομικό δελτίο, εκτιμάται σε [44 451 000 EUR]).