ΕΥΡΩΠΑΪΚΗ
ΕΠΙΤΡΟΠΗ

Βρυξέλλες, 4.10.2017
COM(2017) 477 final

2017/0225 (COD)

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 477 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 477 final/2 of 4.10.2017

Πρόταση

ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

σχετικά με τον ENISA, τον «οργανισμό της ΕΕ για την ασφάλεια στον κυβερνοχώρο», και την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013, καθώς και σχετικά με την πιστοποίηση της ασφάλειας στον κυβερνοχώρο στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών («πράξη για την ασφάλεια στον κυβερνοχώρο»)

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

{SWD(2017) 500 final}
{SWD(2017) 501 final}
{SWD(2017) 502 final}

ΑΙΤΙΟΛΟΓΙΚΗ ΕΚΘΕΣΗ

1. ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΤΑΣΗΣ

- **Αιτιολόγηση και στόχοι της πρότασης**

Η Ευρωπαϊκή Ένωση έχει αναλάβει σειρά δράσεων για την αύξηση της ανθεκτικότητας και την ενίσχυση της ετοιμότητάς της σε ζητήματα ασφάλειας στον κυβερνοχώρο. Η πρώτη Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο[1] που εγκρίθηκε το 2013 καθορίζει στρατηγικούς στόχους και συγκεκριμένες δράσεις για την επίτευξη ανθεκτικότητας, τη μείωση του ηλεκτρονικού εγκλήματος, την επεξεργασία πολιτικής και ανάπτυξη ικανοτήτων για την άμυνα στον κυβερνοχώρο, την ανάπτυξη βιομηχανικών και τεχνολογικών πόρων και τη θέσπιση συνεκτικής διεθνούς πολιτικής κυβερνοχώρου για την ΕΕ. Στο πλαίσιο αυτό, έκτοτε σημειώθηκαν σημαντικές εξελίξεις, συμπεριλαμβανομένης ιδίως της δεύτερης εντολής του Οργανισμού της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA)[2] και της έκδοσης της **οδηγίας για την ασφάλεια συστημάτων δικτύου και πληροφοριών**[3] (η «οδηγία NIS»), που συνιστούν τη βάση της παρούσας πρότασης.

Επιπλέον, το **2016 η Ευρωπαϊκή Επιτροπή εξέδωσε ανακοίνωση σχετικά με την ενίσχυση του συστήματος κυβερνοανθεκτικότητας της Ευρώπης και προώθηση ανταγωνιστικού και καινοτόμου κλάδου ασφάλειας στον κυβερνοχώρο**[4], στην οποία ανακοινώθηκαν περαιτέρω μέτρα για την αναβάθμιση της συνεργασίας και ανταλλαγής πληροφοριών και γνώσεων και την ενίσχυση της ανθεκτικότητας και της ετοιμότητας της ΕΕ, λαμβανομένου επίσης υπόψη του ενδεχόμενου συμβάντων μεγάλης κλίμακας και μιας ενδεχόμενης πανευρωπαϊκής κρίσης ασφάλειας στον κυβερνοχώρο. Στο πλαίσιο αυτό, η Επιτροπή ανακοίνωσε ότι θα προωθήσει την **αξιολόγηση** και **αναθεώρηση** του κανονισμού (ΕΕ) αριθ. 526/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τον ENISA και την κατάργηση του κανονισμού (ΕΚ) αριθ. 460/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου («κανονισμός ENISA»). Η διαδικασία αξιολόγησης ενδέχεται να οδηγήσει σε πιθανή μεταρρύθμιση του Οργανισμού και ενίσχυση των δυνατοτήτων και ικανοτήτων του να υποστηρίζει τα κράτη μέλη κατά τρόπο βιώσιμο. Θα προσέδιδε επομένως πιο επιχειρησιακό και κεντρικό ρόλο στην επίτευξη ανθεκτικότητας σχετικά με την ασφάλεια στον κυβερνοχώρο και θα αναγνώριζε στη νέα εντολή του Οργανισμού τις νέες του αρμοδιότητες σύμφωνα με την οδηγία NIS.

Η οδηγία NIS είναι το πρώτο σημαντικό βήμα με στόχο την προαγωγή νοοτροπίας διαχείρισης κινδύνου, μέσω της θέσπισης απαιτήσεων ασφαλείας ως νόμιμες υποχρεώσεις για τους βασικούς οικονομικούς φορείς, ιδίως τους φορείς που παρέχουν βασικές υπηρεσίες

---

[1] Κοινή ανακοίνωση της Ευρωπαϊκής Επιτροπής και της Ευρωπαϊκής Υπηρεσίας Εξωτερικής Δράσης: Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο: Για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο - JOIN(2013).

[2] Κανονισμός (ΕΕ) αριθ. 526/2013 σχετικά με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) και την κατάργηση του κανονισμού (ΕΚ) αριθ. 460/2004

[3] Οδηγία (ΕΕ) 2016/1148 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση

[4] Ανακοίνωση της Επιτροπής σχετικά με την ενίσχυση του συστήματος κυβερνοανθεκτικότητας της Ευρώπης και προώθηση ανταγωνιστικού και καινοτόμου κλάδου ασφάλειας στον κυβερνοχώρο, COM/2016/0410 final.

(φορείς εκμετάλλευσης βασικών υπηρεσιών – ΦΒΥ) και τους παρόχους ορισμένων βασικών ψηφιακών υπηρεσιών (παρόχους ψηφιακών υπηρεσιών – ΠΨΥ). Καθώς οι απαιτήσεις ασφαλείας θεωρούνται σημαντικές για τη διαφύλαξη των πλεονεκτημάτων της εξελισσόμενης ψηφιοποίησης της κοινωνίας και δεδομένης της ταχείας διάδοσης των συνδεδεμένων συσκευών (το διαδίκτυο των πραγμάτων), η ανακοίνωση του 2016 προήγαγε επίσης την ιδέα θέσπισης πλαισίου για την πιστοποίηση της ασφάλειας των προϊόντων και υπηρεσιών ΤΠΕ, προκειμένου να ενισχυθεί η εμπιστοσύνη και η ασφάλεια στην ψηφιακή ενιαία αγορά. Η πιστοποίηση της ασφάλειας στον κυβερνοχώρο των ΤΠΕ καθίσταται ιδιαίτερα σημαντική ενόψει της αυξημένης χρήσης τεχνολογιών που απαιτούν υψηλό επίπεδο ασφάλειας στον κυβερνοχώρο, όπως π.χ. τα συνδεδεμένα και αυτοματοποιημένα αυτοκίνητα, τα ηλεκτρονικά συστήματα υγείας ή τα συστήματα βιομηχανικού αυτοματισμού και ελέγχου (IACS).

Τα εν λόγω μέτρα πολιτικής και ανακοινώσεις ενισχύθηκαν περαιτέρω με τα **συμπεράσματα του Συμβουλίου** του 2016, με τα οποία αναγνωρίστηκε ότι «οι απειλές και τα ευάλωτα σημεία στον κυβερνοχώρο εξακολουθούν να αυξάνονται και να εντείνονται, πράγμα που θα απαιτήσει συνεχή και στενότερη συνεργασία, ιδίως στο πλαίσιο της αντιμετώπισης διασυνοριακών συμβάντων ασφάλειας στον κυβερνοχώρο μεγάλης κλίμακας». Στα συμπεράσματα επιβεβαιώθηκε ότι ο κανονισμός ENISA αποτελεί μία από «τις βασικές συνιστώσες ενός πλαισίου της ΕΕ για την ανθεκτικότητα στον κυβερνοχώρο»[5] και κλήθηκε η Επιτροπή να λάβει περαιτέρω μέτρα για την αντιμετώπιση του ζητήματος της πιστοποίησης σε ευρωπαϊκό επίπεδο.

Η θέσπιση συστήματος πιστοποίησης απαιτεί τη δημιουργία κατάλληλου συστήματος διακυβέρνησης σε επίπεδο ΕΕ που θα περιλαμβάνει εμπειρογνωμοσύνη που παρέχεται από ανεξάρτητο οργανισμό της ΕΕ. Από την άποψη αυτή, η παρούσα πρόταση προσδιορίζει τον ENISA ως τον φυσικό αρμόδιο φορέα σε επίπεδο ΕΕ για την ασφάλεια στον κυβερνοχώρο που θα αναλάβει να συγκεντρώσει και να συντονίσει τις εργασίες των εθνικών αρμόδιων φορέων στον τομέα της πιστοποίησης.

Στην ανακοίνωσή της σχετικά με την **ενδιάμεση επανεξέταση της εφαρμογής της στρατηγικής για την ψηφιακή ενιαία αγορά**, η Επιτροπή διευκρίνισε περαιτέρω ότι έως τον Σεπτέμβριο του 2017 θα επανεξετάσει την εντολή του ENISA. Αυτό θα γίνει προκειμένου να καθοριστεί ο ρόλος του στο μεταβαλλόμενο οικοσύστημα ασφάλειας στον κυβερνοχώρο και να αναπτυχθούν μέτρα σχετικά με τα πρότυπα ασφάλειας, την πιστοποίηση και την επισήμανση στον κυβερνοχώρο, με σκοπό να ενισχυθεί η ασφάλεια στον κυβερνοχώρο των συστημάτων που βασίζονται σε ΤΠΕ, συμπεριλαμβανομένων των συνδεδεμένων αντικειμένων[6]. Το **Ευρωπαϊκό Συμβούλιο, στα συμπεράσματά του** τον Ιούνιο του 2017[7] χαιρέτισε την πρόθεση της Επιτροπής να επανεξετάσει τη Στρατηγική για την ασφάλεια στον κυβερνοχώρο και να προτείνει περαιτέρω στοχευμένες δράσεις πριν το τέλος του 2017.

Ο προτεινόμενος κανονισμός προβλέπει ολοκληρωμένη σειρά μέτρων που βασίζονται σε προηγούμενες δράσεις και ευνοεί την αμοιβαία ενίσχυση συγκεκριμένων στόχων:

---

5 Συμπεράσματα του Συμβουλίου σχετικά με την ενίσχυση του ευρωπαϊκού συστήματος ανθεκτικότητας στον κυβερνοχώρο και την προώθηση ενός ανταγωνιστικού και καινοτόμου κλάδου κυβερνοασφάλειας - 15 Νοεμβρίου 2016.

6 Ανακοίνωση της Επιτροπής σχετικά με την ενδιάμεση επανεξέταση της εφαρμογής της στρατηγικής για την ψηφιακή ενιαία αγορά - COM(2017) 228.

7 Σύνοδος του Ευρωπαϊκού Συμβουλίου (22 και 23 Ιουνίου 2017) – Συμπεράσματα, EUCO 8/17.

- αύξηση των **ικανοτήτων και της ετοιμότητας** των κρατών μελών και των επιχειρήσεων·

- βελτίωση της **συνεργασίας και του συντονισμού** στα κράτη μέλη και τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ·

- αύξηση των **ικανοτήτων σε επίπεδο ΕΕ για τη συμπλήρωση της δράσης των κρατών μελών**, ιδίως στην περίπτωση των διασυνοριακών κρίσεων στον κυβερνοχώρο·

- αύξηση της **ευαισθητοποίησης** των πολιτών και των επιχειρήσεων σε ζητήματα ασφάλειας στον κυβερνοχώρο·

- αύξηση της συνολικής **διαφάνειας της διασφάλισης της ασφάλειας στον κυβερνοχώρο**[8] των προϊόντων και υπηρεσιών ΤΠΕ με σκοπό την ενίσχυση της εμπιστοσύνης στην ψηφιακή ενιαία αγορά και την ψηφιακή καινοτομία και

- αποφυγή του **κατακερματισμού των συστημάτων πιστοποίησης** στην ΕΕ και των σχετικών απαιτήσεων ασφαλείας και κριτηρίων αξιολόγησης μεταξύ κρατών μελών και τομέων.

Το παρακάτω μέρος της αιτιολογικής έκθεσης εξηγεί με περισσότερη λεπτομέρεια το σκεπτικό για την πρωτοβουλία σε σχέση με τις προτεινόμενες δράσεις για τον ENISA και την πιστοποίηση της ασφάλειας στον κυβερνοχώρο.

[8] Ως διαφάνεια της διασφάλισης της ασφάλειας στον κυβερνοχώρο ορίζεται η παροχή στους χρήστες επαρκών πληροφοριών σχετικά με τις ιδιότητες ασφάλειας στον κυβερνοχώρο, γεγονός που επιτρέπει στους χρήστες να προσδιορίσουν με αντικειμενικό τρόπο το επίπεδο ασφάλειας ενός δεδομένου προϊόντος, υπηρεσίας ή διαδικασίας ΤΠΕ.

ENISA

Ο ENISA ενεργεί ως κέντρο εμπειρογνωσίας με ρόλο την προαγωγή της ασφάλειας των δικτύων και των πληροφοριών στην Ένωση και τη στήριξη της ανάπτυξης ικανοτήτων των κρατών μελών.

Ο ENISA δημιουργήθηκε το 2004[9] με σκοπό να συμβάλλει στη διασφάλιση υψηλού επιπέδου ασφάλειας των δικτύων και των πληροφοριών εντός της ΕΕ. Το 2013, με τον κανονισμό (ΕΕ) αριθ. 526/2013 θεσπίστηκε η νέα εντολή του Οργανισμού για διάστημα επτά ετών, έως το 2020. Τα γραφεία του Οργανισμού βρίσκονται στην Ελλάδα και συγκεκριμένα, η διοικητική του έδρα στο Ηράκλειο (Κρήτη) και το επιχειρησιακό του κέντρο στην Αθήνα.

Ο ENISA είναι μικρός οργανισμός με χαμηλό προϋπολογισμό και αριθμό προσωπικού σε σχέση με όλους τους οργανισμούς της ΕΕ. Έχει εντολή καθορισμένου χρόνου.

Ο ENISA στηρίζει τα ευρωπαϊκά θεσμικά όργανα, τα κράτη μέλη και την επιχειρηματική κοινότητα στην **αντιμετώπιση και ιδίως την πρόληψη προβλημάτων σε σχέση με την ασφάλεια των δικτύων και των πληροφοριών**. Αυτό επιτυγχάνεται μέσω σειράς δραστηριοτήτων σε πέντε τομείς που προσδιορίζονται στη στρατηγική του[10]:

- Εμπειρογνωσία: η παροχή πληροφοριών και εμπειρογνωσίας σχετικά με βασικά ζητήματα ασφαλείας δικτύων και πληροφοριών.
- Πολιτική: η στήριξη της χάραξης πολιτικής και της εφαρμογής της στην Ένωση.
- Ικανότητα: η στήριξη της ανάπτυξης ικανοτήτων στην Ένωση (π.χ. μέσω δράσεων κατάρτισης, συστάσεων, δραστηριοτήτων ευαισθητοποίησης).
- Κοινότητα: η ενίσχυση της κοινότητας ασφάλειας δικτύων και πληροφοριών (π.χ. στήριξη των ομάδων αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT), συντονισμός των πανευρωπαϊκών κυβερνοασκήσεων).
- Αποτελεσματική υποστήριξη (π.χ. επαφή με τους άμεσα ενδιαφερόμενους και διεθνείς σχέσεις).

Κατά την πορεία των διαπραγματεύσεων για την οδηγία NIS, οι συννομοθέτες της ΕΕ αποφάσισαν να αναγνωρίσουν σημαντικό ρόλο στον ENISA για την εφαρμογή της οδηγίας. Συγκεκριμένα, ο Οργανισμός παρέχει γραμματειακή υποστήριξη στο δίκτυο CSIRT (που έχει δημιουργηθεί για την προαγωγή της ταχείας και αποτελεσματικής επιχειρησιακής συνεργασίας μεταξύ των κρατών μελών σε συγκεκριμένα συμβάντα που αφορούν την ασφάλεια στον κυβερνοχώρο και την ανταλλαγή πληροφοριών σχετικά με τους κινδύνους), και καλείται επίσης να βοηθήσει την ομάδα συνεργασίας στην εκτέλεση των καθηκόντων της. Επιπλέον, η οδηγία προβλέπει ότι ο ENISA θα πρέπει να στηρίζει τα κράτη μέλη και την Επιτροπή, παρέχοντας την εμπειρογνωμοσύνη και τις συμβουλές του, καθώς και διευκολύνοντας την ανταλλαγή βέλτιστων πρακτικών.

---

9 Κανονισμός (ΕΚ) αριθ. 460/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 10ης Μαρτίου 2004, για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια δικτύων και Πληροφοριών, ΕΕ L 77 της 13.3.2004, σ. 1.

10 https://www.enisa.europa.eu/publications/corporate/enisa-strategy

Σύμφωνα με τον κανονισμό ENISA, η Επιτροπή έχει διενεργήσει αξιολόγηση του Οργανισμού που περιλαμβάνει ανεξάρτητη μελέτη καθώς και δημόσια διαβούλευση. Αντικείμενο της αξιολόγησης ήταν η συνάφεια, ο αντίκτυπος, η αποτελεσματικότητα, η αποδοτικότητα, η συνοχή και η προστιθέμενη αξία της ΕΕ του οργανισμού σε σχέση με την επίδοση, τη διακυβέρνηση, την εσωτερική οργανωτική δομή και τις εργασιακές πρακτικές του κατά την περίοδο 2013-2016.

Η συνολική επίδοση του ENISA αξιολογήθηκε θετικά από την πλειονότητα των απαντησάντων[11] (74 %) στη δημόσια διαβούλευση. Επιπλέον, οι περισσότεροι από τους απαντήσαντες θεώρησαν ότι ο ENISA επιτυγχάνει τους διαφορετικούς στόχους του (τουλάχιστον 63 % για κάθε στόχο). Οι υπηρεσίες και τα προϊόντα του ENISA χρησιμοποιούνται τακτικά (κάθε μήνα ή πιο συχνά) από το ήμισυ σχεδόν των απαντησάντων (46 %) και χαίρουν εκτίμησης καθώς προέρχονται από όργανο σε επίπεδο ΕΕ (83 %) και για την ποιότητά τους (62 %).

Ωστόσο, στη σημαντική τους πλειοψηφία (88 %), οι απαντήσαντες θεώρησαν ότι τα υφιστάμενα μέσα και μηχανισμοί που είναι διαθέσιμα σε επίπεδο ΕΕ είναι ανεπαρκή ή μόνο εν μέρει επαρκή για την αντιμετώπιση των υφιστάμενων προκλήσεων όσον αφορά την ασφάλεια στον κυβερνοχώρο. Στη συντριπτική τους πλειοψηφία (98 %), οι απαντήσαντες ανέφεραν ότι οι εν λόγω ανάγκες θα πρέπει να αντιμετωπιστούν από οργανισμό της ΕΕ και το 99 % των απαντησάντων θεώρησε ότι ο ENISA είναι η κατάλληλη οργάνωση για αυτό μεταξύ των εν λόγω οργανισμών. Επιπλέον, το 67,5 % των απαντησάντων εξέφρασε την άποψη ότι ο ENISA θα μπορούσε να παίξει ρόλο στη θέσπιση εναρμονισμένου πλαισίου για την πιστοποίηση της ασφάλειας προϊόντων και υπηρεσιών ΤΠ.

Από τη συνολική αξιολόγηση (βάσει όχι μόνο της δημόσιας διαβούλευσης αλλά και σειράς ατομικών συνεντεύξεων, επιπλέον στοχοθετημένων ερευνών και εργαστηρίων) προέκυψαν τα παρακάτω συμπεράσματα:

- Οι στόχοι του ENISA παραμένουν συναφείς και σήμερα. Στο πλαίσιο των ραγδαίων τεχνολογικών εξελίξεων και των εξελισσόμενων απειλών και ενόψει των αυξανόμενων κινδύνων για την ασφάλεια στον κυβερνοχώρο σε παγκόσμιο επίπεδο, είναι σαφής η ανάγκη στην ΕΕ για προαγωγή και περαιτέρω ενίσχυση της υψηλού επιπέδου τεχνικής εμπειρογνωμοσύνης σε ζητήματα ασφάλειας στον κυβερνοχώρο. Είναι απαραίτητη η οικοδόμηση ικανοτήτων στα κράτη μέλη για την κατανόηση και την αντιμετώπιση των απειλών και η συνεργασία των άμεσα ενδιαφερόμενων μεταξύ θεματικών πεδίων και οργανισμών.

- Παρά τον χαμηλό του προϋπολογισμό, ο Οργανισμός είναι επιχειρησιακά αποτελεσματικός στη χρήση των πόρων του και την εκτέλεση των καθηκόντων του. Ωστόσο, ο διαχωρισμός των εγκαταστάσεών του μεταξύ Αθήνας και Ηρακλείου είχε ως αποτέλεσμα περαιτέρω διοικητικό κόστος.

- Όσον αφορά την αποτελεσματικότητά του, ο ENISA πέτυχε εν μέρει τους στόχους του. Ο Οργανισμός συνέβαλε επιτυχώς στη βελτίωση της ασφάλειας δικτύων και πληροφοριών στην Ευρώπη μέσω της προσφοράς ανάπτυξης ικανοτήτων σε 28

[11] 90 άμεσα ενδιαφερόμενοι από 19 κράτη μέλη απάντησαν στη διαβούλευση (88 απαντήσεις και 2 έγγραφα θέσεων), συμπεριλαμβανομένων των εθνικών αρχών 15 κρατών μελών και 8 κεντρικών οργανώσεων που αντιπροσωπεύουν σημαντικό αριθμό ευρωπαϊκών επιχειρήσεων.

κράτη μέλη[12], της ενίσχυσης της συνεργασίας μεταξύ κρατών μελών και άμεσα ενδιαφερόμενων για την ασφάλεια δικτύων και πληροφοριών και μέσω της παροχής εμπειρογνωσίας, ανάπτυξης της κοινότητας και υποστήριξης για την ανάπτυξη πολιτικών. Συνολικά, ο ENISA επικεντρώθηκε επιμελώς στην υλοποίηση του προγράμματος εργασίας του και ενήργησε ως έμπιστος εταίρος για τους άμεσα ενδιαφερόμενους, σε έναν τομέα που μόλις πρόσφατα αναγνωρίστηκε ότι παρουσιάζει τόσο έντονο διασυνοριακό ενδιαφέρον.

- Ο ENISA κατάφερε να έχει αντίκτυπο, τουλάχιστον σε ορισμένο βαθμό, στο ευρύ πεδίο της ασφάλειας δικτύων και πληροφοριών, ωστόσο δεν έχει πετύχει απόλυτα στην ανάπτυξη ισχυρής επωνυμίας και την εξασφάλιση επαρκούς προβολής ώστε να είναι αναγνωρίσιμος ως το βασικό κέντρο εμπειρογνωσίας στην Ευρώπη. Αυτό εξηγείται από την ευρεία εντολή του ENISA που δεν διαθέτει αναλογικά επαρκείς πόρους. Επιπλέον, ο ENISA παραμένει ο μοναδικός οργανισμός της ΕΕ με εντολή καθορισμένου χρόνου, γεγονός που περιορίζει την ικανότητά του να αναπτύξει μακροπρόθεσμο όραμα και να υποστηρίξει τους άμεσα ενδιαφερόμενους κατά τρόπο βιώσιμο. Αυτό έρχεται επίσης σε αντίθεση με τις διατάξεις της οδηγίας NIS που επιφορτίζουν τον ENISA με καθήκοντα χωρίς καταληκτική ημερομηνία. Τέλος, από την αξιολόγηση προέκυψε ότι η περιορισμένη αυτή αποτελεσματικότητα εξηγείται εν μέρει από τη μεγάλη εξάρτηση από την εξωτερική εμπειρογνωσία σε σχέση με την εμπειρογνωσία που είναι διαθέσιμη εντός του οργανισμού και από τις δυσκολίες στην προσέλκυση και διατήρηση εξειδικευμένου προσωπικού.

- Τέλος, και εξίσου σημαντικό, από την αξιολόγηση προέκυψε ότι η προστιθέμενη αξία του ENISA πηγάζει πρωτίστως από την ικανότητα του Οργανισμού να ενισχύει τη συνεργασία κυρίως μεταξύ των κρατών μελών και ειδικά με συναφείς κοινότητες για την ασφάλεια δικτύων και πληροφοριών (και συγκεκριμένα μεταξύ CSIRT). Δεν υπάρχει άλλος φορέας σε επίπεδο ΕΕ που να στηρίζει τόσο ευρύ φάσμα άμεσα ενδιαφερόμενων για την ασφάλεια δικτύων και πληροφοριών. Ωστόσο, λόγω της ανάγκης για αυστηρή προτεραιότητα στις δραστηριότητές του, το πρόγραμμα εργασίας του ENISA βασίζεται κυρίως στις ανάγκες των κρατών μελών. Ως αποτέλεσμα, δεν αντιμετωπίζει επαρκώς τις ανάγκες των άλλων άμεσα ενδιαφερόμενων, ιδίως στον κλάδο. Οδήγησε επίσης τον Οργανισμό στην εκ των υστέρων ικανοποίηση των αναγκών των κύριων άμεσα ενδιαφερόμενων, με αποτέλεσμα να μην μπορεί να έχει μεγαλύτερο αντίκτυπο. Επομένως, η προστιθέμενη αξία που προσφέρει ο Οργανισμός ποίκιλλε ανάλογα με τις διαφορετικές ανάγκες των άμεσα ενδιαφερόμενων και στον βαθμό που ο Οργανισμός μπορούσε να ανταποκριθεί σε αυτές (π.χ. μεγάλα έναντι μικρών κρατών μελών· κράτη μέλη έναντι του κλάδου).

[12] Οι απαντήσαντες στο πλαίσιο της δημόσιας διαβούλευσης κλήθηκαν να σχολιάσουν ποια θεωρούσαν τα σημαντικότερα επιτεύγματα του ENISA στο διάστημα 2013-2016. Οι απαντήσαντες από όλες τις ομάδες (συνολικά 55, 13 εκ των οποίων από εθνικές αρχές, 20 από τον ιδιωτικό τομέα και 22 «άλλοι») θεώρησαν ότι τα παρακάτω αποτελούσαν τα σημαντικότερα επιτεύγματα του ENISA: 1) ο συντονισμός των ασκήσεων Cyber Europe· 2) η παροχή στήριξης στις CERT/CSIRT μέσω κατάρτισης και εργαστηρίων για την προαγωγή του συντονισμού και της ανταλλαγής απόψεων· 3) οι δημοσιεύσεις του ENISA (κατευθυντήριες οδηγίες και συστάσεις, εκθέσεις για τη φύση των απειλών, στρατηγικές για την αναφορά περιστατικών και τη διαχείριση κρίσεων, κλπ.) που θεωρήθηκαν χρήσιμες για τη δημιουργία και την επικαιροποίηση των εθνικών πλαισίων ασφαλείας, καθώς και ως πηγή αναφοράς για τους χαράκτες πολιτικής και τους επαγγελματίες που δραστηριοποιούνται στον κυβερνοχώρο· 4) η συμβολή στην προώθηση της οδηγίας NIS· 5) οι προσπάθειες αύξησης της ευαισθητοποίησης σχετικά με την ασφάλεια στον κυβερνοχώρο μέσω του μήνα για την ασφάλεια στον κυβερνοχώρο.

Με λίγα λόγια, τα αποτελέσματα των διαβουλεύσεων με τους άμεσα ενδιαφερόμενους και της αξιολόγησης δείχνουν ότι οι πόροι και η εντολή του ENISA πρέπει να προσαρμοστούν ώστε να μπορέσει να διαδραματίσει επαρκή ρόλο στην αντιμετώπιση των υφιστάμενων και μελλοντικών προκλήσεων.

Με βάση αυτά τα ευρήματα, η παρούσα πρόταση επανεξετάζει την τρέχουσα εντολή του ENISA και καθορίζει ανανεωμένη σειρά καθηκόντων και λειτουργιών, με σκοπό την αποτελεσματική και αποδοτική υποστήριξη των κρατών μελών, των θεσμικών οργάνων της ΕΕ και των προσπαθειών άλλων άμεσα ενδιαφερόμενων για τη διασφάλιση ασφαλούς κυβερνοχώρου στην Ευρωπαϊκή Ένωση. Στόχος της νέας προτεινόμενης εντολής είναι να προσδώσει στον Οργανισμό ισχυρότερο και πιο κεντρικό ρόλο, κυρίως με τη στήριξη και των κρατών μελών στην εφαρμογή της οδηγίας NIS και την αντιμετώπιση συγκεκριμένων απειλών πιο ενεργά (επιχειρησιακή ικανότητα) και με τη μετατροπή του σε κέντρο εμπειρογνωσίας για τη στήριξη των κρατών μελών και της Επιτροπής σε θέματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο. Βάσει της παρούσας πρότασης:

- Ο ENISA θα λάβει μόνιμη εντολή και επομένως θα έχει σταθερή βάση για το μέλλον. Η εντολή, οι στόχοι και τα καθήκοντά του θα πρέπει να υπόκεινται ακόμη σε τακτική επανεξέταση.

- Η προτεινόμενη εντολή διευκρινίζει περαιτέρω τον ρόλο του ENISA ως τον οργανισμό της ΕΕ για την ασφάλεια στον κυβερνοχώρο και ως σημείο αναφοράς στο οικοσύστημα της ΕΕ για την ασφάλεια στον κυβερνοχώρο, που συνεργάζεται στενά με όλους τους άλλους σχετικούς φορείς του εν λόγω οικοσυστήματος.

- Η οργάνωση και η διακυβέρνηση του Οργανισμού, που έλαβαν θετικές κριτικές κατά την αξιολόγηση, θα επανεξεταστούν συγκρατημένα, ιδίως προκειμένου να διασφαλιστεί ότι οι ανάγκες της ευρύτερης κοινότητας των άμεσα ενδιαφερόμενων αποτυπώνονται καλύτερα στο έργο του Οργανισμού.

- Οριοθετείται το προτεινόμενο εύρος της εντολής, που ενισχύει τους τομείς στους οποίους έχει καταστεί σαφές ότι ο Οργανισμός παράγει προστιθέμενη αξία και προσθέτει τους νέους εκείνους τομείς που χρήζουν στήριξης με βάση τις νέες προτεραιότητες και μέσα πολιτικής, συγκεκριμένα την οδηγία NIS, την επανεξέταση της Στρατηγικής της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο, το επερχόμενο προσχέδιο της ΕΕ για την ασφάλεια στον κυβερνοχώρο εν όψει της συνεργασίας στην αντιμετώπιση των κρίσεων στον κυβερνοχώρο, και την πιστοποίηση ασφαλείας ΤΠΕ:

    - **Χάραξη και εφαρμογή πολιτικής της ΕΕ:** Ο ENISA θα αναλάβει να συμβάλλει ενεργά στη χάραξη πολιτικής στον τομέα της ασφάλειας δικτύων πληροφοριών, καθώς και σε άλλες πρωτοβουλίες πολιτικής που εμπεριέχουν στοιχεία ασφάλειας στον κυβερνοχώρο σε διαφορετικούς τομείς (π.χ. της ενέργειας, των μεταφορών, τον οικονομικών). Για τον σκοπό αυτό θα έχει ισχυρό συμβουλευτικό ρόλο τον οποίο θα μπορεί να εκπληρώνει με την παροχή ανεξάρτητων γνωμοδοτήσεων και προπαρασκευαστικές εργασίες για την ανάπτυξη και επικαιροποίηση της πολιτικής και της νομοθεσίας. Ο ENISA θα στηρίζει επίσης την πολιτική και τη νομοθεσία της ΕΕ στους τομείς των ηλεκτρονικών επικοινωνιών, της ηλεκτρονικής ταυτοποίησης και των υπηρεσιών εμπιστοσύνης με σκοπό την προαγωγή ενισχυμένου επιπέδου ασφάλειας στον κυβερνοχώρο. Στο στάδιο της εφαρμογής, ιδίως στο πλαίσιο

της ομάδας συνεργασίας της οδηγίας NIS, ο ENISA θα επικουρεί τα κράτη μέλη στην επίτευξη συνεκτικής προσέγγισης στην εφαρμογή της οδηγίας NIS σε διασυνοριακό και διατομεακό επίπεδο, καθώς και σε άλλες σχετικές πολιτικές και νόμους. Προκειμένου να στηρίξει την τακτική επανεξέταση πολιτικών και νόμων στον τομέα της ασφάλειας στον κυβερνοχώρο, ο ENISA θα υποβάλλει τακτικά εκθέσεις σχετικά με την κατάσταση της εφαρμογής του νομικού πλαισίου της ΕΕ.

- **Ανάπτυξη ικανοτήτων:** Ο ENISA θα συνεισφέρει στη βελτίωση των ικανοτήτων και της εμπειρογνωσίας των αρχών της ΕΕ και των εθνικών δημόσιων αρχών, ιδίως στην αντιμετώπιση συμβάντων και την επίβλεψη των κανονιστικών μέτρων που σχετίζονται με την ασφάλεια στον κυβερνοχώρο. Ο Οργανισμός θα πρέπει επίσης να συνεισφέρει στη δημιουργία κέντρων κοινοχρησίας και ανάλυσης πληροφοριών (ISAC) σε διάφορους τομείς, με την παροχή βέλτιστων πρακτικών και καθοδήγησης σχετικά με τα διαθέσιμα εργαλεία και τις διαδικασίες, καθώς και με την κατάλληλη αντιμετώπιση κανονιστικών ζητημάτων που σχετίζονται με την ανταλλαγή πληροφοριών.

- **Γνώση και πληροφορίες, ευαισθητοποίηση:** Ο ENISA θα μετατραπεί σε κόμβο ανταλλαγής πληροφοριών της ΕΕ. Αυτό συνεπάγεται την προώθηση και την ανταλλαγή βέλτιστων πρακτικών και πρωτοβουλιών σε όλη την ΕΕ με τη συγκέντρωση πληροφοριών σχετικά με την ασφάλεια στον κυβερνοχώρο, οι οποίες προέρχονται από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ. Ο Οργανισμός θα προσφέρει επίσης συμβουλές, καθοδήγηση και βέλτιστες πρακτικές σχετικά με την ασφάλεια των υποδομών ζωτικής σημασίας. Επιπλέον, μετά από σημαντικά διασυνοριακά συμβάντα που αφορούν την ασφάλεια στον κυβερνοχώρο ο ENISA θα συντάσσει εκθέσεις με σκοπό την παροχή καθοδήγησης στις επιχειρήσεις και τους πολίτες σε όλη την ΕΕ. Στις εργασίες αυτές θα περιλαμβάνεται επίσης η τακτική οργάνωση δραστηριοτήτων ευαισθητοποίησης σε συνεργασία με τις αρχές των κρατών μελών.

- **Καθήκοντα σχετικά με την αγορά (τυποποίηση, πιστοποίηση της ασφάλειας στον κυβερνοχώρο):** Ο ENISA θα εκτελεί σειρά λειτουργιών για τη στήριξη ειδικότερα της εσωτερικής αγοράς και θα συντονίζει «παρατηρητήριο αγοράς» για την ασφάλεια στον κυβερνοχώρο, μέσω της ανάλυσης των σχετικών τάσεων στην αγορά της ασφάλειας στον κυβερνοχώρο ώστε να υπάρχει επιτευχθεί μεγαλύτερη αντιστοιχία ζήτησης και προσφοράς και μέσω της στήριξης της χάραξης πολιτικής της ΕΕ στους τομείς της τυποποίησης ΤΠΕ και της πιστοποίησης της ασφάλειας στον κυβερνοχώρο των ΤΠΕ. Όσον αφορά συγκεκριμένα την τυποποίηση, θα διευκολύνει τη θέσπιση και την αξιοποίηση προτύπων για την ασφάλεια στον κυβερνοχώρο. Ο ENISA θα εκτελεί επίσης τα καθήκοντα που προβλέπονται στο μελλοντικό πλαίσιο για την πιστοποίηση (βλ. παρακάτω τμήμα).

- **Έρευνα και καινοτομία:** Ο ENISA θα προσφέρει την εμπειρογνωσία του μέσω της παροχής συμβουλών στις αρχές της ΕΕ και τις εθνικές αρχές σχετικά με τον καθορισμό προτεραιοτήτων στους τομείς της έρευνας και της ανάπτυξης, συμπεριλαμβανομένου του πλαισίου της σύμπραξης δημόσιου-ιδιωτικού τομέα για την ασφάλεια στον κυβερνοχώρο (cPPP). Οι συμβουλές του ENISA σχετικά με την έρευνα θα τροφοδοτούν το νέο Ευρωπαϊκό Κέντρο

Έρευνας και Ικανοτήτων για την ασφάλεια στον κυβερνοχώρο με βάση το επόμενο πολυετές δημοσιονομικό πλαίσιο. Ο ENISA θα συμμετέχει, όταν του ζητείται από την Επιτροπή, στην υλοποίηση προγραμμάτων χρηματοδότησης της ΕΕ για την έρευνα και την καινοτομία.

- **Επιχειρησιακή συνεργασία και διαχείριση κρίσεων:** Οι εργασίες αυτές θα πρέπει να βασίζονται στην ενίσχυση των υφιστάμενων προληπτικών επιχειρησιακών ικανοτήτων, ιδίως την αναβάθμιση των πανευρωπαϊκών ασκήσεων για την ασφάλεια στον κυβερνοχώρο (Cyber Europe) με τη διεξαγωγή τους σε ετήσια βάση, και στον υποστηρικτικό ρόλο στην επιχειρησιακή συνεργασία με την παροχή γραμματειακής υποστήριξης στο δίκτυο CSIRT (σύμφωνα με τις διατάξεις της οδηγίας NIS) μέσω της διασφάλισης, μεταξύ άλλων, της ορθής λειτουργίας της υποδομής ΤΠ και των διαύλων επικοινωνίας του δικτύου CSIRT. Στο πλαίσιο αυτό, θα είναι απαραίτητη η διαρθρωμένη συνεργασία με την CERT-EU, το European Cybercrime Centre (EC3) και άλλους σχετικούς φορείς της ΕΕ. Επιπλέον, η διαρθρωμένη συνεργασία με την CERT-EU, σε μικρή φυσική απόσταση, θα πρέπει να έχει ως αποτέλεσμα μια λειτουργία για την παροχή τεχνικής υποστήριξης σε περίπτωση σημαντικών συμβάντων και την υποστήριξη της ανάλυσης συμβάντων. Τα κράτη μέλη θα μπορούν να ζητήσουν βοήθεια για την αντιμετώπιση συμβάντων και στήριξη για την ανάλυση τρωτών σημείων, σφαλμάτων και συμβάντων με σκοπό την ενίσχυση της προληπτικής τους ικανότητας και της ικανότητας αντίδρασής τους.

- Ο ENISA θα διαδραματίσει επίσης ρόλο στο **προσχέδιο της ΕΕ για την ασφάλεια στον κυβερνοχώρο** που παρουσιάστηκε στο πλαίσιο του εν λόγω πακέτου και καθορίζει τις συστάσεις της Επιτροπής προς τα κράτη μέλη για συντονισμένη αντιμετώπιση σε επίπεδο ΕΕ των μεγάλης κλίμακας διασυνοριακών συμβάντων και κρίσεων που αφορούν την ασφάλεια στον κυβερνοχώρο[13]. Ο ENISA θα διευκολύνει τη συνεργασία μεταξύ μεμονωμένων κρατών μελών για την αντιμετώπιση έκτακτων αναγκών μέσω της ανάλυσης και της συγκέντρωσης εθνικών εκθέσεων κατάστασης που βασίζονται στις πληροφορίες που διατίθενται στον Οργανισμό σε εθελοντική βάση από τα κράτη μέλη και άλλες οντότητες.

- **Πιστοποίηση της ασφάλειας στον κυβερνοχώρο προϊόντων και υπηρεσιών ΤΠΕ**

Για την εδραίωση και τη διατήρηση της εμπιστοσύνης, τα προϊόντα και οι υπηρεσίες ΤΠΕ πρέπει να ενσωματώνουν απευθείας χαρακτηριστικά ασφαλείας στα αρχικά στάδια του τεχνικού τους σχεδιασμού και ανάπτυξης (ασφάλεια βάσει σχεδιασμού). Επιπλέον, οι πελάτες και οι χρήστες πρέπει να είναι σε θέση να βεβαιώνουν το επίπεδο διασφάλισης της ασφάλειας των προϊόντων και των υπηρεσιών που προμηθεύονται ή αγοράζουν.

Η πιστοποίηση, που αποτελείται από την επίσημη αξιολόγηση των προϊόντων, υπηρεσιών και διαδικασιών από ανεξάρτητο και πιστοποιημένο φορέα βάσει καθορισμένης δέσμης

[13] Το «προσχέδιο» θα έχει εφαρμογή σε συμβάντα που αφορούν την ασφάλεια στον κυβερνοχώρο τα οποία προκαλούν διαταραχές τέτοιας έκτασης που κανένα κράτος μέλος δεν μπορεί να αντιμετωπίσει από μόνο του ή που επηρεάζουν δύο ή περισσότερα κράτη μέλη με τόσο ευρύ και σημαντικό αντίκτυπο ή πολιτική σημασία που απαιτούν έγκαιρο συντονισμό πολιτικής και αντιμετώπιση σε πολιτικό επίπεδο Ένωσης.

πρότυπων κριτηρίων και την έκδοση πιστοποιητικού που βεβαιώνει τη συμμόρφωση, διαδραματίζει σημαντικό ρόλο στην αύξηση της εμπιστοσύνης και της ασφάλειας των προϊόντων και των υπηρεσιών. Αν και η αξιολόγηση της ασφάλειας αποτελεί ιδιαιτέρως τεχνικό τομέα, η πιστοποίηση εξυπηρετεί την ενημέρωση και τη διαβεβαίωση των αγοραστών και των χρηστών σχετικά με τις ιδιότητες ασφαλείας των προϊόντων και υπηρεσιών ΤΠΕ που αγοράζουν ή χρησιμοποιούν. Όπως προαναφέρθηκε, αυτό ισχύει ιδίως για τα νέα συστήματα στα οποία χρησιμοποιούνται εκτενώς ψηφιακές τεχνολογίες και τα οποία απαιτούν υψηλό επίπεδο ασφάλειας, όπως π.χ. τα συνδεδεμένα και αυτοματοποιημένα αυτοκίνητα, τα ηλεκτρονικά συστήματα υγείας, τα συστήματα βιομηχανικού αυτοματισμού και ελέγχου (IACS)[14] ή τα έξυπνα δίκτυα.

Επί του παρόντος, το τοπίο της πιστοποίησης της ασφάλειας στον κυβερνοχώρο προϊόντων και υπηρεσιών ΤΠΕ στην ΕΕ παρουσιάζει αρκετές διαφοροποιήσεις. Υπάρχει σειρά διεθνών πρωτοβουλιών, όπως τα λεγόμενα κοινά κριτήρια (ΚΚ) για την αξιολόγηση της ασφάλειας της τεχνολογίας πληροφοριών (ISO 15408) που αποτελεί διεθνές πρότυπο για την αξιολόγηση της ασφάλειας των ηλεκτρονικών υπολογιστών. Βασίζεται στην αξιολόγηση από τρίτους και προβλέπει επτά επίπεδα διασφάλισης της αξιολόγησης (EAL). Τα ΚΚ και η συνοδευτική κοινή μεθοδολογία για την αξιολόγηση της ασφάλειας της τεχνολογίας πληροφοριών (ΚΜ) αποτελούν την τεχνική βάση για διεθνή συμφωνία, τη συμφωνία για την αναγνώριση κοινών κριτηρίων (ΣΑΚΚ) που διασφαλίζει ότι τα πιστοποιητικά ΚΚ αναγνωρίζονται από όλα τα μέρη που υπογράφουν τη ΣΑΚΚ. Ωστόσο, στην παρούσα έκδοση της ΣΑΚΚ αναγνωρίζονται αμοιβαία μόνο αξιολογήσεις έως το επίπεδο EAL 2. Επιπλέον, μόνο 13 κράτη μέλη έχουν υπογράψει τη συμφωνία.

Οι αρχές πιστοποίησης 12 κρατών μελών έχουν συνάψει συμφωνία αμοιβαίας αναγνώρισης σχετικά με τα πιστοποιητικά που εκδίδονται σύμφωνα με τις διατάξεις της συμφωνίας, βάσει των κοινών κριτηρίων[15]. Επιπλέον, επί του παρόντος υφίστανται ή είναι υπό θέσπιση αρκετές πρωτοβουλίες πιστοποίησης ΤΠΕ στα κράτη μέλη. Αν και σημαντικές, οι εν λόγω πρωτοβουλίες ενέχουν τον κίνδυνο να κατακερματίσουν την αγορά και να δημιουργήσουν προβλήματα διαλειτουργικότητας. Ως αποτέλεσμα, μια εταιρεία μπορεί να χρειαστεί να υποβληθεί σε αρκετές διαδικασίες πιστοποίησης σε διάφορα κράτη μέλη προκειμένου να μπορέσει να προσφέρει το προϊόν της σε περισσότερες αγορές. Για παράδειγμα, ένας κατασκευαστής έξυπνων μετρητών που θέλει να πωλήσει τα προϊόντα του σε τρία κράτη μέλη, π.χ. τη Γερμανία, τη Γαλλία και το ΗΒ, πρέπει επί του παρόντος να συμμορφωθεί με τρία διαφορετικά συστήματα πιστοποίησης. Στο ΗΒ υπάρχει το σύστημα Commercial Product Assurance (CPA), στη Γαλλία το Certification de Sécurité de Premier Niveau (CSPN) και στη Γερμανία ειδικό προφίλ προστασίας που βασίζεται στα κοινά κριτήρια.

---

[14] Η ΓΔ JRC έχει δημοσιεύσει έκθεση με την οποία προτείνεται αρχική δέσμη κοινών ευρωπαϊκών απαιτήσεων και γενικών κατευθυντήριων γραμμών σχετικών με την πιστοποίηση ασφάλειας στον κυβερνοχώρο των συστατικών στοιχείων των IACS. Διατίθεται στον δικτυακό τόπο: https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf

[15] Η Ομάδα Ανωτέρων Υπαλλήλων για την Ασφάλεια των Συστημάτων Πληροφοριών (SOG-IS) περιλαμβάνει 12 κράτη μέλη, καθώς και τη Νορβηγία, και έχει αναπτύξει ορισμένα προφίλ προστασίας για περιορισμένο αριθμό προϊόντων όπως η ψηφιακή υπογραφή, ο ψηφιακός ταχογράφος και οι έξυπνες κάρτες. Οι συμμετέχοντες εργάζονται από κοινού για τον συντονισμό της τυποποίησης των προφίλ προστασίας του ΚΚ και τον συντονισμό της ανάπτυξης προφίλ προστασίας. Τα κράτη μέλη συχνά ζητούν πιστοποίηση από τη SOG-IS για εθνικούς διαγωνισμούς για την ανάθεση δημοσίων συμβάσεων.

Η κατάσταση αυτή οδηγεί σε υψηλότερα έξοδα και συνιστά σημαντικό διοικητικό φόρτο για τις εταιρείες που δραστηριοποιούνται σε περισσότερα κράτη μέλη. Αν και το κόστος της πιστοποίησης μπορεί να διαφέρει σημαντικά, ανάλογα με το υπό εξέταση προϊόν/υπηρεσία, το επίπεδο διασφάλισης της αξιολόγησης που επιδιώκεται και/ή άλλα στοιχεία, τείνει να είναι αρκετά σημαντικό για τις επιχειρήσεις. Για παράδειγμα, για το πιστοποιητικό της υπηρεσίας BSI «Smart Meter Gateway», το κόστος ανέρχεται σε πάνω από 1 εκατ. EUR (υψηλότερο επίπεδο δοκιμής και διασφάλισης, αφορά όχι μόνο ένα προϊόν αλλά και το σύνολο της υποδομής γύρω από αυτό). Το κόστος για την πιστοποίηση έξυπνων μετρητών στο HB ανέρχεται σε σχεδόν 150 000 EUR. Στη Γαλλία το κόστος είναι παρόμοιο με του HB και ανέρχεται σε περίπου 150 000 EUR ή παραπάνω.

Βασικοί άμεσα ενδιαφερόμενοι του δημόσιου και του ιδιωτικού τομέα αναγνώρισαν ότι ελλείψει συστήματος πιστοποίησης της ασφάλειας στον κυβερνοχώρο σε επίπεδο ΕΕ, οι εταιρίες αναγκάζονται σε πολλές περιπτώσεις να λάβουν χωριστή πιστοποίηση σε κάθε κράτος μέλος, με αποτέλεσμα τον κατακερματισμό της αγοράς. Το σημαντικότερο, ελλείψει νομοθεσίας εναρμόνισης της ΕΕ για τα προϊόντα και τις υπηρεσίες ΤΠΕ, οι διαφορές στα πρότυπα και οι πρακτικές πιστοποίησης της ασφάλειας στον κυβερνοχώρο στα κράτη μέλη ενδέχεται να οδηγήσουν στην πράξη στη δημιουργία 28 χωριστών αγορών ασφάλειας στην ΕΕ, καθεμία εκ των οποίων θα έχει τις δικές τις τεχνικές απαιτήσεις, μεθόδους δοκιμής και διαδικασίες πιστοποίησης της ασφάλειας στον κυβερνοχώρο. Οι αποκλίνουσες αυτές προσεγγίσεις σε εθνικό επίπεδο ενδέχεται να αποτελέσουν – εφόσον δεν ληφθούν επαρκή μέτρα σε επίπεδο ΕΕ – σημαντικό ανασταλτικό παράγοντα για την επίτευξη της ψηφιακής ενιαίας αγοράς, καθυστερώντας ή και αποτρέποντας τον συνδεδεμένο θετικό αντίκτυπο όσον αφορά την ανάπτυξη και την απασχόληση.

Βάσει των παραπάνω εξελίξεων, ο προτεινόμενος κανονισμός θεσπίζει ευρωπαϊκό πλαίσιο πιστοποίησης της ασφάλειας στον κυβερνοχώρο (το «**πλαίσιο**») για προϊόντα και υπηρεσίες ΤΠΕ και καθορίζει τις βασικές λειτουργίες και καθήκοντα του ENISA στον τομέα της πιστοποίησης της ασφάλειας στον κυβερνοχώρο. Η παρούσα πρόταση προβλέπει συνολικό πλαίσιο κανόνων που διέπουν τα ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο. Η πρόταση δεν θεσπίζει άμεσα εφαρμόσιμα συστήματα πιστοποίησης, αλλά δημιουργεί ένα σύστημα (πλαίσιο) για τη θέσπιση συγκεκριμένων συστημάτων πιστοποίησης για συγκεκριμένα προϊόντα/υπηρεσίες ΤΠΕ (τα «ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο»). Η δημιουργία ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο σύμφωνα με το πλαίσιο θα επιτρέψει την έκδοση πιστοποιητικών βάσει των εν λόγω συστημάτων τα οποία θα είναι έγκυρα και αναγνωρισμένα σε όλα τα κράτη μέλη, και την αντιμετώπιση του σημερινού κατακερματισμού της αγοράς.

Ο γενικός σκοπός των ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο είναι να βεβαιώνουν ότι τα προϊόντα και οι υπηρεσίες ΤΠΕ που έχουν πιστοποιηθεί σύμφωνα με τα συστήματα αυτά συμμορφώνονται με τις καθορισμένες απαιτήσεις ασφάλειας στον κυβερνοχώρο. Αυτό περιλαμβάνει για παράδειγμα την ικανότητά τους να προστατεύουν δεδομένα (που αποθηκεύτηκαν, διαβιβάστηκαν ή υπέστησαν άλλη επεξεργασία) από την τυχαία ή μη εγκεκριμένη αποθήκευση, επεξεργασία, πρόσβαση, κοινοποίηση, καταστροφή, τυχαία απώλεια ή αλλοίωσή τους. Τα συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο της ΕΕ θα αξιοποιούν τα υφιστάμενα πρότυπα όσον αφορά τις τεχνικές απαιτήσεις και τις διαδικασίες αξιολόγησης με τις οποίες πρέπει να

συμμορφώνονται τα προϊόντα και δεν θα αναπτύσσουν τα εν λόγω πρότυπα τα ίδια[16]. Για παράδειγμα, πιστοποίηση σε επίπεδο ΕΕ προϊόντων όπως οι έξυπνες κάρτες που δοκιμάζονται σήμερα με βάση τα διεθνή πρότυπα ΚΚ στο πλαίσιο του πολυμερούς συστήματος SOG-IS (και περιγράφονται παραπάνω) θα καθιστούσε το εν λόγω σύστημα έγκυρο σε όλη την ΕΕ.

Πέρα από την περιγραφή συγκεκριμένης δέσμης στόχων ασφαλείας που πρέπει να λαμβάνονται υπόψη στον σχεδιασμό συγκεκριμένου ευρωπαϊκού συστήματος πιστοποίησης της ασφάλειας στον κυβερνοχώρο, η πρόταση προβλέπει το ελάχιστο περιεχόμενο που θα έπρεπε να έχουν τα εν λόγω συστήματα. Τα συστήματα αυτά θα πρέπει να καθορίζουν, μεταξύ άλλων, σειρά συγκεκριμένων στοιχείων που θα ορίζουν το πεδίο εφαρμογής και το αντικείμενο της πιστοποίησης της ασφάλειας στον κυβερνοχώρο. Αυτό περιλαμβάνει τον προσδιορισμό των κατηγοριών προϊόντων και υπηρεσιών που καλύπτονται, τον λεπτομερή καθορισμό των απαιτήσεων ασφάλειας στον κυβερνοχώρο (για παράδειγμα, με αναφορά στα σχετικά πρότυπα ή τεχνικές προδιαγραφές), τα συγκεκριμένα κριτήρια και μεθόδους αξιολόγησης και το επίπεδο διασφάλισης που προορίζονται να εξασφαλίσουν (δηλαδή, βασικό, ουσιαστικό ή υψηλό).

Τα ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο θα προετοιμάζονται από τον ENISA με τη βοήθεια, την εμπειρογνωσία και τη στενή συνεργασία της ευρωπαϊκής ομάδας πιστοποίησης της ασφάλειας στον κυβερνοχώρο (βλ. παρακάτω) και θα εγκρίνονται από την Επιτροπή μέσω εκτελεστικών πράξεων. Όταν διαπιστώνεται η ανάγκη για σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο, η Επιτροπή θα ζητά από τον ENISA να ετοιμάσει σύστημα για συγκεκριμένα προϊόντα ή υπηρεσίες ΤΠΕ. Ο ENISA θα προετοιμάζει το σύστημα σε στενή συνεργασία με εθνικές εποπτικές αρχές πιστοποίησης που εκπροσωπούνται στην ομάδα. Τα κράτη μέλη και η ομάδα δύνανται να προτείνουν στην Επιτροπή να ζητήσει από τον ENISA την προετοιμασία ορισμένου συστήματος.

Η πιστοποίηση μπορεί να είναι πολύ ακριβή διαδικασία που με τη σειρά της θα μπορούσε να οδηγήσει σε υψηλότερες τιμές για τους πελάτες και τους καταναλωτές. Η ανάγκη για πιστοποίηση μπορεί επίσης να διαφέρει σημαντικά ανάλογα με το συγκεκριμένο πλαίσιο χρήσης των προϊόντων και υπηρεσιών και τον γρήγορο ρυθμό των τεχνολογικών εξελίξεων. Η προσφυγή σε ευρωπαϊκή πιστοποίηση της ασφάλειας στον κυβερνοχώρο θα πρέπει επομένως να παραμείνει προαιρετική, εκτός αν προβλέπεται άλλως στην ενωσιακή νομοθεσία που θεσπίζει απαιτήσεις ασφάλειας για τα προϊόντα και τις υπηρεσίες ΤΠΕ.

Προκειμένου να εξασφαλιστεί η εναρμόνιση και να αποφευχθεί ο κατακερματισμός, τα εθνικά συστήματα ή οι διαδικασίες πιστοποίησης της ασφάλειας στον κυβερνοχώρο για τα προϊόντα και τις υπηρεσίες ΤΠΕ που καλύπτονται από ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο θα παύουν να ισχύουν από την ημερομηνία που ορίζεται στην εκτελεστική πράξη με την οποία θεσπίζεται το ευρωπαϊκό σύστημα. Τα κράτη μέλη θα πρέπει επιπλέον, να μην θεσπίζουν νέα εθνικά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο για τα προϊόντα και τις υπηρεσίες ΤΠΕ που καλύπτονται από ήδη υφιστάμενο ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο.

[16] Στην περίπτωση των ευρωπαϊκών προτύπων, αυτό επιτυγχάνεται μέσω των ευρωπαϊκών οργανισμών τυποποίησης και εγκρίνεται από την Ευρωπαϊκή Επιτροπή με δημοσίευση στην *Επίσημη Εφημερίδα* (βλ. κανονισμό αριθ. 1025/2012).

Από τη στιγμή που ένα ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο εγκριθεί, οι κατασκευαστές προϊόντων ΤΠΕ ή οι πάροχοι υπηρεσιών ΤΠΕ θα μπορούν να υποβάλλουν αίτηση για την πιστοποίηση των προϊόντων ή των υπηρεσιών τους σε οργανισμό αξιολόγησης της συμμόρφωσης της επιλογής τους. Οι οργανισμοί αξιολόγησης της συμμόρφωσης θα πρέπει να είναι διαπιστευμένοι από οργανισμό διαπίστευσης αν συμμορφώνονται με ορισμένες συγκεκριμένες απαιτήσεις. Η διαπίστευση θα χορηγείται για μέγιστη περίοδο πέντε ετών και μπορεί να ανανεωθεί με τους ίδιους όρους, υπό την προϋπόθεση ότι ο οργανισμός αξιολόγησης της συμμόρφωσης πληροί τις σχετικές απαιτήσεις. Οι οργανισμοί διαπίστευσης θα ανακαλούν τη διαπίστευση οργανισμού αξιολόγησης της συμμόρφωσης στις περιπτώσεις που οι όροι για τη διαπίστευση δεν πληρούνται ή δεν πληρούνται πλέον ή που οι ενέργειες του οργανισμού αξιολόγησης της συμμόρφωσης παραβαίνουν τον παρόντα κανονισμό.

Σύμφωνα με την πρόταση, τα κράτη μέλη είναι επιφορτισμένα με καθήκοντα παρακολούθησης, εποπτείας και επιβολής. Τα κράτη μέλη θα πρέπει να συστήσουν εποπτική αρχή πιστοποίησης. Η αρχή αυτή θα είναι επιφορτισμένη με την εποπτεία της συμμόρφωσης των οργανισμών αξιολόγησης της συμμόρφωσης, καθώς και των πιστοποιητικών που εκδίδονται από τους οργανισμούς αξιολόγησης της συμμόρφωσης που έχουν συσταθεί στην επικράτειά της, σύμφωνα με τις απαιτήσεις του παρόντος κανονισμού και των σχετικών ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο. Οι εθνικές εποπτικές αρχές πιστοποίησης θα είναι αρμόδιες για την εξέταση καταγγελιών που υποβάλλονται από φυσικά ή νομικά πρόσωπα σε σχέση με πιστοποιητικά που εκδίδονται από οργανισμούς αξιολόγησης της συμμόρφωσης που έχουν συσταθεί στην επικράτειά τους. Θα εξετάζουν στον ενδεδειγμένο βαθμό το αντικείμενο της καταγγελίας και θα ενημερώνουν τον καταγγέλλοντα σχετικά με την πρόοδο και το αποτέλεσμα της έρευνας εντός εύλογου χρονικού διαστήματος. Επιπλέον, θα συνεργάζονται με άλλες εποπτικές αρχές πιστοποίησης ή άλλες δημόσιες αρχές, π.χ. με την ανταλλαγή πληροφοριών σχετικά με την πιθανή μη συμμόρφωση προϊόντων και υπηρεσιών ΤΠΕ με τις απαιτήσεις του παρόντος κανονισμού ή με τα συγκεκριμένα ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο.

Τέλος, η πρόταση θεσπίζει την ευρωπαϊκή ομάδα πιστοποίησης της ασφάλειας στον κυβερνοχώρο (η «ομάδα») που αποτελείται από τις εθνικές εποπτικές αρχές πιστοποίησης όλων των κρατών μελών. Κύριο καθήκον της ομάδας είναι να συμβουλεύει την Επιτροπή για ζητήματα σχετικά με την πολιτική πιστοποίησης της ασφάλειας στον κυβερνοχώρο και να συνεργάζεται με τον ENISA για την ανάπτυξη σχεδίων ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο. Ο ENISA θα επικουρεί την Επιτροπή στην παροχή γραμματειακής υποστήριξης στην ομάδα και θα διατηρεί ενημερωμένο δημόσιο κατάλογο συστημάτων που έχουν εγκριθεί βάσει του ευρωπαϊκού πλαισίου πιστοποίησης της ασφάλειας στον κυβερνοχώρο. Ο ENISA θα συνεργάζεται επίσης με οργανισμούς τυποποίησης για τη διασφάλιση της καταλληλότητας των προτύπων που χρησιμοποιούνται στα εγκεκριμένα συστήματα και τον προσδιορισμό τομέων που χρήζουν προτύπων για την ασφάλεια στον κυβερνοχώρο.

Το ευρωπαϊκό πλαίσιο πιστοποίησης της ασφάλειας στον κυβερνοχώρο («πλαίσιο») θα προσφέρει αρκετά οφέλη για τους πολίτες και τις επιχειρήσεις. Ειδικότερα:

- Η δημιουργία συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο σε επίπεδο ΕΕ για συγκεκριμένα προϊόντα ή υπηρεσίες θα δώσει στις εταιρείες μια υπηρεσία μίας στάσης για την πιστοποίηση της ασφάλειας στον κυβερνοχώρο στην ΕΕ. Οι εταιρείες αυτές θα μπορούν να πιστοποιούν τα προϊόντα τους μόνο άπαξ και να αποκτούν πιστοποιητικό που θα είναι έγκυρο σε όλα τα κράτη μέλη. Δεν θα

υποχρεούνται να πιστοποιήσουν εκ νέου τα προϊόντα τους σε διαφορετικούς εθνικούς φορείς πιστοποίησης. Αυτό θα μειώσει σημαντικά το κόστος για τις εταιρείες, θα διευκολύνει τις διασυνοριακές δραστηριότητες και θα μειώσει και αποτρέψει εν τέλει τον κατακερματισμό της εσωτερικής αγοράς για τα υπό εξέταση προϊόντα.

- Το πλαίσιο εδραιώνει την υπεροχή των ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο έναντι των εθνικών συστημάτων: σύμφωνα με τον εν λόγω κανόνα, η θέσπιση ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο θα υπερισχύει έναντι όλων των υφιστάμενων παράλληλων εθνικών συστημάτων για τα ίδια προϊόντα ή υπηρεσίες ΤΠΕ σε ορισμένο επίπεδο διασφάλισης. Αυτό θα ενισχύσει τη σαφήνεια, με τη μείωση της τρέχουσας διάδοσης αλληλεπικαλυπτόμενων και ενδεχομένως αντικρουόμενων εθνικών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο.

- Η πρόταση στηρίζει και συμπληρώνει την εφαρμογή της οδηγίας NIS παρέχοντας στις εταιρείες που εμπίπτουν στην οδηγία ένα πολύ χρήσιμο εργαλείο για την απόδειξη της συμμόρφωσης με τις απαιτήσεις της σε όλη την Ένωση. Με την ανάπτυξη νέων συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο, η Επιτροπή και ο ENISA θα δώσουν ιδιαίτερη προσοχή στην ανάγκη να εξασφαλιστεί ότι οι απαιτήσεις της οδηγίας NIS αποτυπώνονται στα συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο.

- Η πρόταση θα στηρίζει και θα διευκολύνει την ανάπτυξη ευρωπαϊκής πολιτικής για την ασφάλεια στον κυβερνοχώρο, μέσω της εναρμόνισης των όρων και των ουσιαστικών απαιτήσεων για την πιστοποίηση της ασφάλειας στον κυβερνοχώρο προϊόντων και υπηρεσιών ΤΠΕ στην ΕΕ. Τα ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο θα αναφέρονται σε κοινά πρότυπα ή κριτήρια αξιολόγησης και μεθόδους δοκιμών. Αυτό θα συμβάλει σημαντικά, αν και έμμεσα, στην εφαρμογή κοινών λύσεων ασφάλειας στην ΕΕ, αίροντας κατ' αυτόν τον τρόπο και τα εμπόδια στην εσωτερική αγορά.

- Το πλαίσιο έχει σχεδιαστεί έτσι ώστε να εξασφαλίζει την απαραίτητη ευελιξία των συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο. Ανάλογα με τις συγκεκριμένες ανάγκες ασφάλειας στον κυβερνοχώρο, ένα προϊόν ή μια υπηρεσία μπορεί να πιστοποιηθεί με βάση υψηλότερα ή χαμηλότερα επίπεδα ασφάλειας. Στον σχεδιασμό των ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο θα λαμβάνεται υπόψη η εν λόγω ευελιξία και κατ' επέκταση τα συστήματα θα προβλέπουν διαφορετικά επίπεδα διασφάλισης (δηλαδή, βασικό, ουσιαστικό ή υψηλό) ώστε να μπορούν να χρησιμοποιηθούν για διαφορετικούς σκοπούς ή σε διαφορετικά πλαίσια.

- Όλα τα παραπάνω στοιχεία θα καταστήσουν την πιστοποίηση της ασφάλειας στον κυβερνοχώρο πιο ελκυστική για τις επιχειρήσεις, ως αποτελεσματικό μέσον για την κοινοποίηση του επιπέδου διασφάλισης της ασφάλειας στον κυβερνοχώρο προϊόντων ή υπηρεσιών ΤΠΕ. Στον βαθμό που η πιστοποίηση της ασφάλειας στον κυβερνοχώρο θα καταστεί λιγότερο δαπανηρή, πιο αποτελεσματική και εμπορικά ελκυστική, οι επιχειρήσεις θα έχουν περισσότερα κίνητρα για την πιστοποίηση των προϊόντων τους έναντι κινδύνων ασφάλειας στον κυβερνοχώρο, συμβάλλοντας έτσι στη διάδοση καλύτερων πρακτικών ασφάλειας στον κυβερνοχώρο στον σχεδιασμό προϊόντων και υπηρεσιών ΤΠΕ (ασφάλεια στον κυβερνοχώρο βάσει σχεδιασμού).

- **Συνοχή με τις ισχύουσες διατάξεις στον τομέα πολιτικής**

Σύμφωνα με την οδηγία NIS, οι φορείς που δραστηριοποιούνται σε τομείς ζωτικούς για την οικονομία και την κοινωνία μας, όπως αυτοί της ενέργειας, των μεταφορών, της ύδρευσης, των τραπεζών, των υποδομών χρηματοπιστωτικών αγορών, της υγείας, της ψηφιακής υποδομής καθώς και των παρόχων ψηφιακών υπηρεσιών (δηλαδή, μηχανές αναζήτησης, υπηρεσίες νεφοϋπολογιστικής και επιγραμμικές αγορές) οφείλουν να λαμβάνουν μέτρα για την κατάλληλη διαχείριση των κινδύνων ασφάλειας. Οι νέοι κανόνες της παρούσας πρότασης συμπληρώνουν και εξασφαλίζουν τη συνοχή με τις διατάξεις της οδηγίας NIS, με σκοπό την περαιτέρω επιδίωξη της ανθεκτικότητας στον κυβερνοχώρο της ΕΕ μέσω ενισχυμένων ικανοτήτων, συνεργασίας, διαχείρισης κινδύνου και ευαισθητοποίησης όσον αφορά τον κυβερνοχώρο.

Επιπλέον, οι κανόνες σχετικά με την πιστοποίηση της ασφάλειας στον κυβερνοχώρο παρέχουν ένα ουσιαστικό εργαλείο για τις εταιρείες που υπάγονται στην οδηγία NIS, καθώς θα έχουν τη δυνατότητα να πιστοποιούν τα προϊόντα και τις υπηρεσίες ΤΠΕ τους έναντι κινδύνων για την ασφάλεια στον κυβερνοχώρο βάσει συστημάτων πιστοποίησης της ασφάλειας στην κυβερνοχώρο που είναι έγκυρα και αναγνωρισμένα σε όλη την ΕΕ. Θα λειτουργούν επίσης συμπληρωματικά ως προς τις απαιτήσεις ασφάλειας που αναφέρονται στον κανονισμό σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης (eIDAS)[17] και την οδηγία για τον ραδιοεξοπλισμό[18].

- **Συνοχή με άλλες πολιτικές της Ένωσης**

Ο κανονισμός (ΕΕ) 2016/679 (ο Γενικός Κανονισμός για την Προστασία Δεδομένων, «**ΓΚΠΔ**»)[19] περιλαμβάνει διατάξεις για τη θέσπιση μηχανισμών πιστοποίησης και σφραγίδων και σημάτων προστασίας των δεδομένων, με σκοπό την απόδειξη της συμμόρφωσης προς τον εν λόγω κανονισμό των πράξεων επεξεργασίας από τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία. Ο παρών κανονισμός ισχύει με την επιφύλαξη της πιστοποίησης των πράξεων επεξεργασίας των δεδομένων, ακόμη και όταν τέτοιες πράξεις βρίσκονται ενσωματωμένες σε προϊόντα και υπηρεσίες, στο πλαίσιο του ΓΚΠΔ.

Ο προτεινόμενος κανονισμός θα διασφαλίσει τη συμβατότητα με τον κανονισμό αριθ. 765/2008 σχετικά με τις απαιτήσεις διαπίστευσης και εποπτείας της αγοράς[20] με παραπομπή στους κανόνες του εν λόγω πλαισίου σχετικά με τους εθνικούς οργανισμούς διαπίστευσης και τους οργανισμούς αξιολόγησης της συμμόρφωσης. Όσον αφορά τις εποπτικές αρχές, ο προτεινόμενος κανονισμός θα απαιτεί από τα κράτη μέλη να ορίσουν εθνικές εποπτικές αρχές

---

17 Κανονισμός (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Ιουλίου 2014, σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ.

18 Οδηγία 2014/53/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Απριλίου 2014, σχετικά με την εναρμόνιση των νομοθεσιών των κρατών μελών σχετικά με τη διαθεσιμότητα ραδιοεξοπλισμού στην αγορά και την κατάργηση της οδηγίας 1999/5/ΕΚ

19 Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (ΕΕ L 119 της 4.5.2016, σ. 1-88).

20 Κανονισμός (ΕΚ) αριθ.765/2008 για τον καθορισμό των απαιτήσεων διαπίστευσης και εποπτείας της αγοράς όσον αφορά την εμπορία των προϊόντων και για την κατάργηση του κανονισμού (ΕΟΚ) αριθ. 339/93 του Συμβουλίου.

πιστοποίησης με καθήκοντα που περιλαμβάνουν την εποπτεία, την παρακολούθηση και την επιβολή των κανόνων. Οι εν λόγω φορείς θα παραμείνουν ξεχωριστοί από τους οργανισμούς αξιολόγησης της συμμόρφωσης, όπως ορίζεται στον κανονισμό αριθ. 765/2008.

2. ΝΟΜΙΚΗ ΒΑΣΗ, ΕΠΙΚΟΥΡΙΚΟΤΗΤΑ ΚΑΙ ΑΝΑΛΟΓΙΚΟΤΗΤΑ

- **Νομική βάση**

Η νομική βάσει για τη δράση της ΕΕ είναι το άρθρο 114 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ) που αφορά την προσέγγιση των νομοθεσιών των κρατών μελών με σκοπό την επίτευξη των στόχων του άρθρου 26 της ΣΛΕΕ, δηλαδή την ορθή λειτουργία της εσωτερικής αγοράς.

Η νομική βάση της εσωτερικής αγοράς για τη σύσταση του ENISA επιβεβαιώθηκε από το Δικαστήριο της Ευρωπαϊκής Ένωσης (στην υπόθεση C-217/04 *Ηνωμένο Βασίλειο κατά Κοινοβουλίου και Συμβουλίου*) και επιβεβαιώθηκε περαιτέρω με τον κανονισμό του 2013 που καθόρισε την τρέχουσα εντολή του Οργανισμού. Επιπλέον, οι δραστηριότητες που αποτυπώνουν τους στόχους της ενίσχυσης της συνεργασίας και του συντονισμού μεταξύ των κρατών μελών και αυτές που προσθέτουν ικανότητες σε επίπεδο ΕΕ για τη συμπλήρωση της δράσης των κρατών μελών θα εμπίπτουν στην κατηγορία της «επιχειρησιακής συνεργασίας». Αυτό αναγνωρίζεται ειδικότερα από την οδηγία NIS (της οποίας νομική βάση είναι το άρθρο 114 της ΣΛΕΕ) ως στόχος στο πλαίσιο του δικτύου CSIRT όπου ο «ENISA παρέχει τη γραμματειακή υποστήριξη και υποστηρίζει ενεργά τη συνεργασία» (άρθρο 12 παράγραφος 2). Ειδικότερα, το άρθρο παράγραφος 3 στοιχείο στ) ορίζει επιπλέον μεταξύ των καθηκόντων του δικτύου CSIRT τον καθορισμό περαιτέρω μορφών επιχειρησιακής συνεργασίας, συμπεριλαμβανομένων μεταξύ άλλων και τα σχετικά με: i) τις κατηγορίες κινδύνων και συμβάντων· ii) τις έγκαιρες προειδοποιήσεις· iii) την αμοιβαία συνδρομή· και iv) τις αρχές και τις λεπτομέρειες για τον συντονισμό, όταν τα κράτη μέλη παρεμβαίνουν για την αντιμετώπιση διασυνοριακών κινδύνων και συμβάντων.

- Ο σημερινός κατακερματισμός των συστημάτων πιστοποίησης για προϊόντα και υπηρεσίες ΤΠΕ είναι επίσης αποτέλεσμα της έλλειψης κοινής, νομικά δεσμευτικά δεσμευτικής και αποτελεσματικής διαδικασίας-πλαίσιο στα κράτη μέλη. Αυτό εμποδίζει τη δημιουργία εσωτερικής αγοράς για προϊόντα και υπηρεσίες ΤΠΕ και θίγει την ανταγωνιστικότητα της ευρωπαϊκής βιομηχανίας στον εν λόγω τομέα. Η παρούσα πρόταση αποσκοπεί στην αντιμετώπιση του υφιστάμενου κατακερματισμού και των σχετικών εμποδίων στην εσωτερική αγορά μέσω της παροχής κοινού πλαισίου για τη θέσπιση συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο που θα είναι έγκυρα σε όλη την ΕΕ.

Επικουρικότητα (σε περίπτωση μη αποκλειστικής αρμοδιότητας)

Η αρχή της επικουρικότητας απαιτεί αξιολόγηση της αναγκαιότητας και της προστιθέμενης αξίας της δράσης της ΕΕ. Ο σεβασμός στην αρχή της επικουρικότητας στον τομέα αυτό είχε ήδη αναγνωριστεί κατά τη θέσπιση του ισχύοντος κανονισμού ENISA[21].

[21] Κανονισμός (ΕΕ) αριθ. 526/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 21ης Μαΐου 2013, σχετικά με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) και την κατάργηση του κανονισμού (ΕΚ) αριθ. 460/2004.

Η ασφάλεια στον κυβερνοχώρο είναι θέμα κοινού ενδιαφέροντος στην Ένωση. Οι αλληλεξαρτήσεις των δικτύων και των συστημάτων πληροφοριών είναι τέτοιες που οι ανεξάρτητοι φορείς (δημόσιοι και ιδιωτικοί, συμπεριλαμβανομένων των πολιτών) συχνά δεν μπορούν να αντιμετωπίσουν τις απειλές και να διαχειριστούν τους κινδύνους και τον πιθανό αντίκτυπο των συμβάντων στον κυβερνοχώρο μεμονωμένα. Από τη μια, οι αλληλεξαρτήσεις σε όλα τα κράτη μέλη, μεταξύ άλλων όσον αφορά τη λειτουργία των υποδομών ζωτικής σημασίας (όπως οι υποδομές στον τομέα της ενέργειας, των μεταφορών, της ύδρευσης, κ.α.), καθιστούν τη δημόσια παρέμβαση σε ευρωπαϊκό επίπεδο όχι μόνο ωφέλιμη αλλά και απαραίτητη. Από την άλλη, η παρέμβαση της ΕΕ μπορεί να έχει θετικό αντίκτυπο λόγω της ανταλλαγής καλών πρακτικών σε όλα τα κράτη μέλη, η οποία μπορεί να οδηγήσει σε ενισχυμένη ασφάλεια στον κυβερνοχώρο στην Ένωση.

Εν ολίγοις, στο τρέχον πλαίσιο και λαμβανομένων υπόψη των μελλοντικών σεναρίων, φαίνεται ότι για την **αύξηση της συλλογικής ανθεκτικότητας της Ένωσης στον κυβερνοχώρο**, δεν επαρκούν **μεμονωμένες ενέργειες από τα κράτη μέλη και μια κατακερματισμένη προσέγγιση στην ασφάλεια στον κυβερνοχώρο.**

Η δράση της ΕΕ θεωρείται επίσης απαραίτητη για την αντιμετώπιση του κατακερματισμού των υφιστάμενων συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο. Θα επέτρεπε στους παραγωγούς να επωφεληθούν πλήρως από μια εσωτερική αγορά, με σημαντική εξοικονόμηση όσον αφορά τα έξοδα δοκιμής και επανασχεδιασμού. Αν και για παράδειγμα η ισχύουσα συμφωνία αμοιβαίας αναγνώρισης (ΣΑΑ) για την Ομάδα Ανωτέρων Υπαλλήλων για την Ασφάλεια των Συστημάτων Πληροφοριών (SOG-IS) έχει επιτύχει σημαντικά αποτελέσματα σε σχέση με το θέμα αυτό, έχει φανεί ότι έχει σημαντικούς περιορισμούς που περιορίζουν την καταλληλότητά της όσον αφορά την παροχή μακροπρόθεσμων βιώσιμων λύσεων για την πλήρη αξιοποίηση των δυνατοτήτων της εσωτερικής αγοράς.

Η προστιθέμενη αξία της δράσης σε επίπεδο ΕΕ, ιδίως για την ενίσχυση της συνεργασίας μεταξύ των κρατών μελών αλλά και μεταξύ των κοινοτήτων για την ασφάλεια δικτύων και πληροφοριών αναγνωρίστηκε με τα συμπεράσματα του Συμβουλίου του 2016[22] και προκύπτει επίσης σαφώς από την αξιολόγηση του ENISA.

- **Αναλογικότητα**

Τα προτεινόμενα μέτρα δεν υπερβαίνουν τα απαιτούμενα για την επίτευξη των στόχων πολιτικής τους. Επιπλέον, το πεδίο της παρέμβασης της ΕΕ δεν εμποδίζει τυχόν περαιτέρω εθνικές δράσεις στον τομέα των θεμάτων εθνικής ασφάλειας. Η δράση της ΕΕ δικαιολογείται επομένως για λόγους επικουρικότητας και αναλογικότητας.

- **Επιλογή του νομικού μέσου**

Με την παρούσα πρόταση αναθεωρείται ο κανονισμός (ΕΕ) αριθ. 526/2013 που καθορίζει την τρέχουσα εντολή και τα καθήκοντα του ENISA. Επιπλέον, λόγω του σημαντικού ρόλου του ENISA στη διαμόρφωση και διαχείριση πλαισίου της ΕΕ για την πιστοποίηση της ασφάλειας στον κυβερνοχώρο, η θέσπιση της νέας εντολής του ENISA και του προαναφερθέντος πλαισίου επιτυγχάνεται καλύτερα με μια ενιαία νομική πράξη με τη μορφή κανονισμού.

[22] Συμπεράσματα του Συμβουλίου σχετικά με την ενίσχυση του ευρωπαϊκού συστήματος ανθεκτικότητας στον κυβερνοχώρο και την προώθηση ενός ανταγωνιστικού και καινοτόμου κλάδου κυβερνοασφάλειας - 15 Νοεμβρίου 2016.

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

Εκ των υστέρων αξιολογήσεις / έλεγχοι καταλληλότητας ισχύουσας νομοθεσίας

Η Επιτροπή, σύμφωνα με τον χάρτη πορείας της αξιολόγησης[23], εξέτασε τη **συνάφεια, τον αντίκτυπο, την αποτελεσματικότητα, την αποδοτικότητα, τη συνοχή και την προστιθέμενη αξία** του Οργανισμού σε σχέση με την επίδοση, τη διακυβέρνηση, την εσωτερική οργανωτική δομή και τις εργασιακές πρακτικές του κατά την περίοδο 2013-2016. Τα κύρια πορίσματα συνοψίζονται ως εξής (για περισσότερα, βλ. το έγγραφο εργασίας των υπηρεσιών της Επιτροπής σχετικά με το θέμα που συνοδεύει την εκτίμηση επιπτώσεων).

- **Συνάφεια:** Στο πλαίσιο των τεχνολογικών εξελίξεων και των εξελισσόμενων απειλών και λαμβανομένης υπόψη της σημαντικής ανάγκης για αυξημένη ασφάλεια στον κυβερνοχώρο στην ΕΕ, οι στόχοι του ENISA αποδείχτηκαν συναφείς. Πράγματι, τα κράτη μέλη και οι φορείς της ΕΕ στηρίζονται στη σημαντική εμπειρογνωσία του σε ζητήματα ασφάλειας στον κυβερνοχώρο. Επιπλέον, είναι απαραίτητη η οικοδόμηση ικανοτήτων στα κράτη μέλη για την καλύτερη κατανόηση και την αντιμετώπιση των απειλών και η συνεργασία των άμεσα ενδιαφερόμενων μεταξύ θεματικών πεδίων και οργανισμών. Η ασφάλεια στον κυβερνοχώρο συνεχίζει να αποτελεί βασική πολιτική προτεραιότητα της ΕΕ στην οποία ο ENISA αναμένεται να ανταποκριθεί· ωστόσο, ο σχεδιασμός του ENISA ως οργανισμού της ΕΕ με εντολή καθορισμένου χρόνου: i) δεν επιτρέπει τον μακροπρόθεσμο σχεδιασμό και τη βιώσιμη στήριξη των κρατών μελών και των θεσμικών οργάνων της ΕΕ· ii) ενδέχεται να οδηγήσει σε νομικό κενό καθώς οι διατάξεις της οδηγίας NIS με τις οποίες ανατίθενται καθήκοντα στον ENISA είναι μόνιμου χαρακτήρα[24]· iii) στερείται συνοχής με όραμα που θα συνδέει τον ENISA με ένα ενισχυμένο οικοσύστημα ασφάλειας στον κυβερνοχώρο της ΕΕ.

- **Αποτελεσματικότητα**: Συνολικά, ο ENISA πέτυχε τους στόχους του και υλοποίησε τα καθήκοντά του. Συνέβαλε στην αύξηση της ασφάλειας δικτύων και πληροφοριών στην Ευρώπη μέσω των βασικών του δραστηριοτήτων (ανάπτυξη ικανοτήτων, παροχή εμπειρογνωσίας, ανάπτυξη της κοινότητας και στήριξη της πολιτικής). Έδειξε, ωστόσο, ότι έχει δυνατότητες βελτίωσης σε κάθε τομέα. Σύμφωνα με την αξιολόγηση, ο ENISA έχει δημιουργήσει ουσιαστικά ισχυρές σχέσεις εμπιστοσύνης με ορισμένους άμεσα ενδιαφερόμενους, ιδίως με τα κράτη μέλη και την κοινότητα CSIRT. Οι παρεμβάσεις στον τομέα της ανάπτυξης ικανοτήτων θεωρήθηκαν αποτελεσματικές ιδίως για τα κράτη μέλη που διαθέτουν περιορισμένους πόρους. Η ενίσχυση της ευρείας συνεργασίας υπήρξε ιδιαίτερα σημαντική, με τους άμεσα ενδιαφερόμενους να συμφωνούν ευρέως για τον θετικό ρόλο που διαδραματίζει ο ENISA στην προσέγγιση ανθρώπων. Ωστόσο, ήταν δύσκολο για τον ENISA να έχει μεγάλο αντίκτυπο στον ευρύτατο τομέα της ασφάλειας δικτύων και πληροφοριών. Αυτό οφειλόταν στο γεγονός ότι είχε μάλλον περιορισμένους ανθρώπινους και οικονομικούς πόρους για την πολύ ευρεία εντολή του. Από την αξιολόγηση προέκυψε επίσης ότι ο ENISA πέτυχε εν μέρει τον στόχο της παροχής

[23] http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_en.pdf

[24] Αναφορά στα άρθρα 7, 9, 11, 12, 19 της οδηγίας για την ασφάλεια συστημάτων δικτύου και πληροφοριών (οδηγία NIS).

εμπειρογνωσίας, καθώς υπήρχαν προβλήματα στην προσέλκυση εμπειρογνωμόνων (βλ. επίσης παρακάτω στο τμήμα περί αποδοτικότητας).

- **Αποδοτικότητα**: Παρά τον μικρό προϋπολογισμό που είχε στη διάθεσή του ο Οργανισμός (από τους μικρότερους σε σχέση με άλλους οργανισμούς της ΕΕ), μπόρεσε να συμβάλει στην επίτευξη στοχοθετημένων στόχων, δείχνοντας συνολική αποδοτικότητα στη χρήση των πόρων του. Σύμφωνα με την αξιολόγηση, οι διαδικασίες ήταν γενικά αποδοτικές και η σαφής οριοθέτηση των καθηκόντων εντός του οργανισμού είχε ως αποτέλεσμα την ορθή εκτέλεση των εργασιών του. Μία από τις βασικές προκλήσεις που αντιμετώπισε ο Οργανισμός σχετικά με την αποδοτικότητά του αφορά τις δυσκολίες που συνάντησε στην προσέλκυση και διατήρηση εμπειρογνωμόνων υψηλού επιπέδου. Τα πορίσματα δείχνουν ότι αυτό εξηγείται από έναν συνδυασμό παραγόντων, συμπεριλαμβανομένων των γενικών δυσκολιών που είχε ο δημόσιος τομέας στο να ανταγωνιστεί τον ιδιωτικό τομέα στην προσπάθεια πρόσληψης εμπειρογνωμόνων υψηλής ειδίκευσης, του τύπου των συμβάσεων (ορισμένου χρόνου) που μπορούσε να προσφέρει κατά κύριο λόγο ο Οργανισμός και του σχετικά χαμηλού επιπέδου ελκυστικότητας του τόπου εγκατάστασης του ENISA, π.χ. λόγω της δυσκολίας που είχαν οι σύζυγοι των εμπειρογνωμόνων στην εύρεση εργασίας. Ο διαχωρισμός των εγκαταστάσεων μεταξύ της Αθήνας και του Ηρακλείου προϋπέθετε επίσης επιπλέον προσπάθειες συντονισμού και είχε ως αποτέλεσμα επιπλέον έξοδα, ωστόσο η μετακίνηση του τμήματος κεντρικών επιχειρήσεων στην Αθήνα το 2013 αύξησε την επιχειρησιακή αποδοτικότητα του Οργανισμού.

- **Συνοχή:** Οι δραστηριότητες του ENISA υπήρξαν γενικά συνεκτικές με τις πολιτικές και τις δραστηριότητες των άμεσα ενδιαφερόμενων, σε εθνικό επίπεδο και σε επίπεδο ΕΕ, ωστόσο απαιτείται πιο συντονισμένη προσέγγιση στην ασφάλεια στον κυβερνοχώρο σε επίπεδο ΕΕ. Η δυνατότητα συνεργασίας μεταξύ ENISA και άλλων φορέων της ΕΕ δεν έχει αξιοποιηθεί πλήρως. Η εξέλιξη στο νομικό και πολιτικό τοπίο της ΕΕ έχει καταστήσει την τρέχουσα εντολή λιγότερο συνεκτική σήμερα.

- **Προστιθέμενη αξία για την ΕΕ**: Η προστιθέμενη αξία του ENISA πηγάζει πρωτίστως από την ικανότητα του Οργανισμού να ενισχύει τη συνεργασία κυρίως μεταξύ των κρατών μελών, αλλά και με συναφείς κοινότητες για την ασφάλεια δικτύων και πληροφοριών. Δεν υπάρχει άλλος φορέας σε επίπεδο ΕΕ που να στηρίζει τη συνεργασία των ίδιων και ποικίλων άμεσα ενδιαφερόμενων για την ασφάλεια δικτύων και πληροφοριών. Η προστιθέμενη αξία που προσφέρει ο Οργανισμός ποίκιλλε ανάλογα με τις διαφορετικές ανάγκες και τους πόρους των άμεσα ενδιαφερόμενων (π.χ. μεγάλα έναντι μικρών κρατών μελών· κράτη μέλη έναντι του κλάδου) και την ανάγκη του Οργανισμού να ιεραρχήσει τις δραστηριότητές του σύμφωνα με το πρόγραμμα εργασίας. Σύμφωνα με την αξιολόγηση, η πιθανή αναστολή της λειτουργίας του ENISA θα αποτελούσε χαμένη ευκαιρία για όλα τα κράτη μέλη. Δεν θα είναι δυνατό να διασφαλιστεί το ίδιο επίπεδο ανάπτυξης της κοινότητας και συνεργασίας σε όλα τα κράτη μέλη στον τομέα της ασφάλειας στον κυβερνοχώρο. Χωρίς έναν πιο κεντρικό οργανισμό της ΕΕ, ο κατακερματισμός θα ήταν μεγαλύτερος και η διμερής ή περιφερειακή συνεργασία θα έπρεπε να συμπληρώσουν το κενό που θα άφηνε ο ENISA.

Σε ό,τι αφορά τις επιδόσεις του ENISA κατά το παρελθόν αλλά και στο μέλλον, οι βασικές τάσεις που προκύπτουν από τη διαβούλευση του 2017 είναι οι ακόλουθες[25]:

- Η συνολική επίδοση του ENISA κατά την περίοδο 2013-2016 αξιολογήθηκε θετικά από τα περισσότερα άτομα που απάντησαν (74 %). Επιπλέον, οι περισσότεροι απαντήσαντες θεώρησαν ότι ο ENISA επιτυγχάνει τους διαφορετικούς στόχους του (τουλάχιστον 63 % για κάθε στόχο). Οι υπηρεσίες και τα προϊόντα του ENISA χρησιμοποιούνται τακτικά (κάθε μήνα ή πιο συχνά) από το ήμισυ σχεδόν των απαντησάντων (46 %) και χαίρουν εκτίμησης καθώς προέρχονται από όργανο σε επίπεδο ΕΕ (83 %) και για την ποιότητά τους (62 %).

- Οι απαντήσαντες προσδιόρισαν σειρά κενών και προκλήσεων για το μέλλον της ασφάλειας στον κυβερνοχώρο στην ΕΕ, με πέντε σημαντικότερα (σε κατάλογο 16) τα παρακάτω: συνεργασία μεταξύ των κρατών μελών· ικανότητα πρόληψης, εντοπισμού και αντιμετώπισης μεγάλης κλίμακας επιθέσεων στον κυβερνοχώρο· συνεργασία μεταξύ των κρατών μελών για ζητήματα που αφορούν την ασφάλεια στον κυβερνοχώρο· συνεργασία και ανταλλαγή πληροφοριών μεταξύ διαφορετικών άμεσα ενδιαφερόμενων, συμπεριλαμβανομένης της συνεργασίας δημόσιου και ιδιωτικού τομέα· προστασία υποδομών ζωτικής σημασίας από επιθέσεις στον κυβερνοχώρο.

- Τα περισσότερα άτομα που απάντησαν (88 %) θεώρησαν ότι τα υφιστάμενα μέσα και μηχανισμοί που είναι διαθέσιμα σε επίπεδο ΕΕ είναι ανεπαρκή ή μόνο εν μέρει επαρκή για την αντιμετώπιση των ανωτέρω. Στη συντριπτική τους πλειοψηφία, οι απαντήσαντες (98 %) ανέφεραν ότι στις εν λόγω ανάγκες θα πρέπει να ανταποκριθεί οργανισμός της ΕΕ και το 99 % αυτών θεώρησαν ότι ο ENISA είναι η κατάλληλη οργάνωση για αυτό μεταξύ των εν λόγω οργανισμών.

Διαβουλεύσεις με τα ενδιαφερόμενα μέρη

- Η Επιτροπή οργάνωσε δημόσια διαβούλευση για την επανεξέταση του ENISA μεταξύ 12 Απριλίου και 5 Ιουλίου του 2106 και έλαβε 421 απαντήσεις[26]. Σύμφωνα με τα αποτελέσματα, το 67,5 % των απαντησάντων εξέφρασε την άποψη ότι ο ENISA θα μπορούσε να διαδραματίσει ρόλο στη θέσπιση εναρμονισμένου πλαισίου για την πιστοποίηση της ασφάλειας προϊόντων και υπηρεσιών ΤΠ.

---

[25] 90 άμεσα ενδιαφερόμενοι από 19 κράτη μέλη απάντησαν στο πλαίσιο της διαβούλευσης (88 απαντήσεις και 2 έγγραφα θέσεων), συμπεριλαμβανομένων των εθνικών αρχών 15 κρατών μελών, μεταξύ των οποίων η Γαλλία, η Ιταλία, η Ιρλανδία και η Ελλάδα και 8 κεντρικές οργανώσεις που αντιπροσωπεύουν σημαντικό αριθμό ευρωπαϊκών οργανώσεων, π.χ. η Ομοσπονδία Ευρωπαϊκών Τραπεζών, η Digital Europe (που αντιπροσωπεύει τη βιομηχανία των ψηφιακών τεχνολογιών στην Ευρώπη), η Ένωση Ευρωπαϊκών Φορέων Εκμετάλλευσης Τηλεπικοινωνιακών Δικτύων (ETNO). Η δημόσια διαβούλευση του ENISA συμπληρώθηκε από διάφορες άλλες πηγές, μεταξύ άλλων: i) διεξοδικές συνεντεύξεις με περίπου 50 βασικούς παράγοντες στην κοινότητα της ασφάλειας στον κυβερνοχώρο· ii) έρευνα στο δίκτυο CSIRT· iii) έρευνα στο διοικητικό συμβούλιο, το εκτελεστικό συμβούλιο, τη μόνιμη ομάδα ενδιαφερομένων του ENISA.

[26] Ελήφθησαν 162 απαντήσεις από πολίτες και 33 από οργανώσεις της κοινωνίας των πολιτών και οργανώσεις καταναλωτών· ελήφθησαν 186 απαντήσεις από εκπροσώπους του κλάδου και 40 από δημόσιες αρχές, συμπεριλαμβανομένων των αρμόδιων αρχών επιβολής της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

Τα αποτελέσματα της διαβούλευσης του 2016 σχετικά με τη σύμπραξη δημόσιου-ιδιωτικού τομέα για την ασφάλεια στον κυβερνοχώρο[27] όσον αφορά το τμήμα περί πιστοποίησης δείχνουν ότι:

- Το 50,4 % (π.χ. 121 από 240) των απαντησάντων δεν γνωρίζει κατά πόσον τα συστήματα εθνικής πιστοποίησης αναγνωρίζονται αμοιβαία σε όλα τα κράτη μέλη της ΕΕ. Το 25,8 % (62 από 240) απάντησαν «όχι», ενώ το 23,8 % (57 από 240) απάντησαν «ναι».

- Το 37,9 % των απαντησάντων (91 από 240) θεωρεί ότι τα υφιστάμενα συστήματα πιστοποίησης δεν υποστηρίζουν τις ανάγκες της ευρωπαϊκής βιομηχανίας. Από την άλλη πλευρά, το 17,5 % (42 από 240) – κυρίως εταιρείες που δραστηριοποιούνται σε παγκόσμιο επίπεδο – εξέφρασε την αντίθετη άποψη.

- Το 49,6 % (119 από 240) των απαντησάντων δηλώνει ότι δεν είναι εύκολο να αποδειχτεί η ισοδυναμία μεταξύ προτύπων, συστημάτων πιστοποίησης και ετικετών. Το 37,9 % (91 από 240) απάντησαν «δεν γνωρίζω», ενώ μόλις το 12,5 % (30 από 240) απάντησαν «ναι».

Συλλογή και χρήση εμπειρογνωσίας

Η Επιτροπή στηρίχθηκε στις ακόλουθες γνώμες ειδικών εξωτερικών συμβούλων:

- Μελέτη με τίτλο Evaluation of ENISA (αξιολόγηση του ENISA) (Ramboll/Carsa 2017· SMART αριθ. 2016/0077),

- Μελέτη με τίτλο ICT Security Certification and Labelling – Evidence gathering and impact assessment (πιστοποίηση της ασφάλειας ΤΠΕ και επισήμανση – συγκέντρωση αποδεικτικών στοιχείων και εκτίμηση επιπτώσεων) (PriceWaterhouseCoopers 2017· SMART αριθ. 2016/0029).

Εκτίμηση επιπτώσεων

- Η έκθεση για την εκτίμηση των επιπτώσεων σχετικά με την παρούσα πρωτοβουλία προσδιόρισε τα παρακάτω βασικά προβλήματα που χρήζουν αντιμετώπισης:

- κατακερματισμός των πολιτικών και των προσεγγίσεων όσον αφορά την ασφάλεια στον κυβερνοχώρο στα κράτη μέλη·

- διασπορά των πόρων και κατακερματισμός των προσεγγίσεων όσον αφορά την ασφάλεια στον κυβερνοχώρο στα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ· και

- ανεπαρκής ευαισθητοποίηση και πληροφόρηση των πολιτών και των εταιρειών, σε συνδυασμό με την αυξανόμενη εμφάνιση πολλών διαφορετικών συστημάτων εθνικής και τομεακής πιστοποίησης.

[27] 240 άμεσα ενδιαφερόμενοι από εθνικές δημόσιες διοικήσεις, μεγάλες επιχειρήσεις, μικρομεσαίες επιχειρήσεις, πολύ μικρές επιχειρήσεις και οργανισμούς ερευνών απάντησαν στην ενότητα περί πιστοποίησης.

Η έκθεση αξιολόγησε τις παρακάτω πιθανές επιλογές όσον αφορά την εντολή του ENISA:

- διατήρηση της υφιστάμενης κατάστασης, δηλαδή διευρυμένη εντολή που θα συνεχίζει να είναι περιορισμένης διάρκειας (βασική επιλογή)·
- λήξη της τρέχουσας εντολής του ENISA, χωρίς ανανέωση, και κατάργηση του ENISA (καμία πολιτική παρέμβαση)·
- «μεταρρύθμιση του ENISA»· και
- δημιουργία οργανισμού της ΕΕ για την ασφάλεια στον κυβερνοχώρο με πλήρη επιχειρησιακή ικανότητα.

Η έκθεση αξιολόγησε τις παρακάτω πιθανές επιλογές όσον αφορά την πιστοποίηση της ασφάλειας στον κυβερνοχώρο:

- καμία πολιτική παρέμβαση (βασική επιλογή)·
- μη νομοθετικά μέτρα (μη δεσμευτικό δίκαιο)·
- νομοθετική πράξη της ΕΕ για τη δημιουργία υποχρεωτικού συστήματος για όλα τα κράτη μέλη που θα βασίζεται στο σύστημα SOG-IS· και
- γενικό πλαίσιο πιστοποίησης της ασφάλειας στον κυβερνοχώρο ΤΠΕ στην ΕΕ.

Η ανάλυση οδήγησε στο συμπέρασμα ότι ένας «μεταρρυθμισμένος ENISA» σε συνδυασμό με ένα γενικό πλαίσιο πιστοποίησης της ασφάλειας στον κυβερνοχώρο των ΤΠΕ στην ΕΕ είναι η προτιμώμενη επιλογή.

Η προτιμώμενη επιλογή αξιολογήθηκε ως η πλέον αποτελεσματική για την ΕΕ για την επίτευξη των παρακάτω καθορισμένων στόχων: αύξηση των ικανοτήτων, της ετοιμότητας, της συνεργασίας, της ευαισθητοποίησης, της διαφάνειας στον τομέα της ασφάλειας στον κυβερνοχώρο και αποφυγή του κατακερματισμού της αγοράς. Έχει επίσης αξιολογηθεί ως η πλέον συνεπής σε σχέση με τις πολιτικές προτεραιότητες της στρατηγικής της ΕΕ για την ασφάλεια στον κυβερνοχώρο και τις σχετικές πολιτικές (π.χ. οδηγία NIS) και τη στρατηγική για την ψηφιακή ενιαία αγορά. Επιπλέον, από τη διαδικασία διαβούλευσης προέκυψε ότι η προτιμώμενη επιλογή έχει τη στήριξη της πλειοψηφίας των άμεσα ενδιαφερόμενων. Επιπλέον, από την ανάλυση που διενεργήθηκε στο πλαίσιο της εκτίμησης επιπτώσεων προέκυψε ότι η προτιμώμενη επιλογή θα επιτύχει τους σχετικούς στόχους μέσω της εύλογης αξιοποίησης πόρων.

Η επιτροπή ρυθμιστικού ελέγχου της Επιτροπής εξέδωσε αρχικά αρνητική γνωμοδότηση στις 24 Ιουλίου και στη συνέχεια θετική γνωμοδότηση στις 25 Αυγούστου 2017 κατόπιν εκ νέου υποβολής. Η τροποποιημένη έκθεση για την εκτίμηση επιπτώσεων περιλάμβανε επιπλέον στοιχεία, τα τελικά συμπεράσματα της αξιολόγησης του ENISA και επιπλέον επεξήγηση των επιλογών πολιτικής και του αντίκτυπού τους. Στο παράρτημα 1 της τελικής έκθεσης για την εκτίμηση επιπτώσεων συνοψίζεται πώς αντιμετωπίστηκαν οι παρατηρήσεις της επιτροπής στη δεύτερη γνωμοδότηση. Συγκεκριμένα, η έκθεση επικαιροποιήθηκε ώστε να παρουσιάζει με μεγαλύτερη λεπτομέρεια το πλαίσιο της ασφάλειας στον κυβερνοχώρο στην ΕΕ, συμπεριλαμβανομένων των μέτρων που περιλαμβάνονται στην κοινή ανακοίνωση με τίτλο «Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ» (JOIN(2017) 450) και έχουν ιδιαίτερη σημασία για τον ENISA: το προσχέδιο της

ΕΕ για την ασφάλεια στον κυβερνοχώρο και το Ευρωπαϊκό Κέντρο Έρευνας και Ικανοτήτων Ασφάλειας στον Κυβερνοχώρο, στο οποίο ο Οργανισμός θα απευθύνεται για συμβουλές όσον αφορά τις ανάγκες έρευνας στην ΕΕ.

Η έκθεση εξηγεί πώς η μεταρρύθμιση του Οργανισμού, συμπεριλαμβανομένων των νέων καθηκόντων, των καλύτερων όρων απασχόλησης και της δομημένης συνεργασίας με τους φορείς της ΕΕ στον τομέα αυτόν θα βελτίωνε την ελκυστικότητά του ως εργοδότη και θα συνέβαλλε στην αντιμετώπιση των προβλημάτων που σχετίζονται με την πρόσληψη εμπειρογνωμόνων. Στο παράρτημα 6 της έκθεσης παρουσιάζεται επίσης αναθεωρημένη εκτίμηση των δαπανών που σχετίζονται με τις επιλογές πολιτικής για τον ENISA. Όσον αφορά το θέμα της πιστοποίησης, η έκθεση αναθεωρήθηκε ώστε να παρέχει λεπτομερέστερες πληροφορίες, συμπεριλαμβανομένης γραφικής αναπαράστασης της προτιμώμενης επιλογής, και ώστε να παρέχει εκτίμηση των δαπανών που σχετίζονται με το νέο πλαίσιο πιστοποίησης για τα κράτη μέλη και την Επιτροπή. Το σκεπτικό για την επιλογή του ENISA ως κύριου φορέα στο πλαίσιο εξηγείται περαιτέρω με βάση την εμπειρογνωσία του στον τομέα και το γεγονός ότι είναι ο μόνος οργανισμός σε επίπεδο ΕΕ όσον αφορά την ασφάλεια στον κυβερνοχώρο. Τέλος, οι ενότητες που αφορούν την πιστοποίηση αναθεωρήθηκαν ώστε να αποσαφηνιστούν πτυχές που σχετίζονται με τη διαφορά με το ισχύον σύστημα SOG-IS, τα οφέλη που σχετίζονται με τις διαφορετικές επιλογές πολιτικής και ώστε να εξηγηθεί το γεγονός ότι ο τύπος του προϊόντος και της υπηρεσίας ΤΠΕ που καλύπτεται από ευρωπαϊκό σύστημα πιστοποίησης θα καθορίζεται στο ίδιο το εγκεκριμένο σύστημα.

Καταλληλότητα του κανονιστικού πλαισίου και απλούστευση

Άνευ αντικειμένου

Επιπτώσεις στα θεμελιώδη δικαιώματα

Η ασφάλεια στον κυβερνοχώρο κατέχει ουσιαστικό ρόλο στην προστασία της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα κάθε προσώπου σύμφωνα με τα άρθρα 7 και 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης. Στην περίπτωση των συμβάντων στον κυβερνοχώρο, η ιδιωτική ζωή και η προστασία των δεδομένων προσωπικού χαρακτήρα εκτίθενται ξεκάθαρα. Επομένως, η ασφάλεια στον κυβερνοχώρο είναι απαραίτητη προϋπόθεση για τον σεβασμό της ιδιωτικής ζωής και της εμπιστευτικότητας των δεδομένων προσωπικού χαρακτήρα. Με βάση αυτή την προοπτική και με στόχο την ενίσχυση της ασφάλειας στον κυβερνοχώρο στην Ευρώπη, η πρόταση προσφέρει σημαντικό συμπλήρωμα στην υφιστάμενη νομοθεσία για την προστασία του θεμελιώδους δικαιώματος στην ιδιωτική ζωή και τα δεδομένα προσωπικού χαρακτήρα. Η ασφάλεια στον κυβερνοχώρο είναι επίσης απαραίτητη για την προστασία της εμπιστευτικότητας των ηλεκτρονικών επικοινωνιών και επομένως για την άσκηση του δικαιώματος ελευθερίας έκφρασης και πληροφόρησης και άλλων συναφών δικαιωμάτων, όπως η ελευθερία σκέψης, συνείδησης και θρησκείας.

4. ΔΗΜΟΣΙΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ

Βλ. δημοσιονομικό δελτίο

5. ΛΟΙΠΑ ΣΤΟΙΧΕΙΑ

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

Η Επιτροπή θα παρακολουθεί την εφαρμογή του κανονισμού και θα υποβάλλει έκθεση αξιολόγησης στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή ανά πενταετία. Οι εκθέσεις αυτές θα είναι δημόσιες και θα περιέχουν λεπτομερή στοιχεία για την αποτελεσματική εφαρμογή και επιβολή του παρόντος κανονισμού.

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

Ο τίτλος Ι του κανονισμού περιέχει τις ακόλουθες γενικές διατάξεις: το αντικείμενο (άρθρο 1), τους ορισμούς (άρθρο 2), συμπεριλαμβανομένων αναφορών σε σχετικούς ορισμούς από άλλα μέσα της ΕΕ, όπως η οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (οδηγία NIS), ο κανονισμός (ΕΚ) αριθ. 765/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τον καθορισμό των απαιτήσεων διαπίστευσης και εποπτείας της αγοράς όσον αφορά την εμπορία των προϊόντων και για την κατάργηση του κανονισμού (ΕΟΚ) αριθ. 339/93 του Συμβουλίου και ο κανονισμός (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ευρωπαϊκή τυποποίηση.

Ο τίτλος ΙΙ του κανονισμού περιέχει βασικές διατάξεις σχετικά με τον ENISA, τον οργανισμό της ΕΕ για την ασφάλεια στον κυβερνοχώρο.

Το κεφάλαιο Ι του εν λόγω τίτλου περιγράφει την εντολή (άρθρο 3), τους στόχους (άρθρο 4) και τα καθήκοντα του Οργανισμού (άρθρα 5 έως 11).

Το κεφάλαιο ΙΙ περιγράφει την οργάνωση του ENISA και περιλαμβάνει βασικές διατάξεις σχετικά με τη δομή του (άρθρο 12). Εξετάζει τη σύνθεση, τους κανόνες ψηφοφορίας και τα καθήκοντα του διοικητικού συμβουλίου (τμήμα 1, άρθρα 13 έως 17), του εκτελεστικού συμβουλίου (τμήμα 2, άρθρο 18) και του εκτελεστικού διευθυντή (τμήμα 3, άρθρο 19). Περιλαμβάνει επίσης διατάξεις σχετικά με τη σύνθεση και τον ρόλο της μόνιμης ομάδας ενδιαφερομένων (τμήμα 4, άρθρο 20). Τέλος, στο τμήμα 5 του εν λόγω κεφαλαίου περιγράφονται οι κανόνες λειτουργίας του Οργανισμού, μεταξύ άλλων και όσον αφορά τον προγραμματισμό των εργασιών του, τη σύγκρουση συμφερόντων, τη διαφάνεια, την τήρηση του απορρήτου και την πρόσβαση σε έγγραφα (άρθρα 21-25).

Το κεφάλαιο ΙΙΙ αφορά την κατάρτιση και τη διάρθρωση του προϋπολογισμού του Οργανισμού (άρθρα 26 και 27), καθώς και κανόνες που διέπουν την εκτέλεσή του (άρθρα 28 και 29). Περιλαμβάνει επίσης διατάξεις που διευκολύνουν την καταπολέμηση της απάτης, της διαφθοράς και άλλων παράνομων πράξεων (άρθρο 30).

Το κεφάλαιο ΙV αφορά τη στελέχωση του Οργανισμού. Περιλαμβάνει γενικές διατάξεις σχετικά με τον κανονισμό υπηρεσιακής κατάστασης και το καθεστώς και τους κανόνες που διέπουν τα προνόμια και τις ασυλίες (άρθρα 31 και 32). Περιέχει επίσης περιγραφή των κανόνων πρόσληψης και διορισμού του εκτελεστικού διευθυντή του Οργανισμού (άρθρο 33). Τέλος, περιλαμβάνει διατάξεις που διέπουν τη χρησιμοποίηση αποσπασμένων εθνικών εμπειρογνωμόνων ή άλλου προσωπικού που δεν απασχολείται από τον Οργανισμό (άρθρο 34).

Τέλος, το κεφάλαιο V περιλαμβάνει τις γενικές διατάξεις που αφορούν τον Οργανισμό. Περιγράφει το νομικό καθεστώς (άρθρο 35) και περιλαμβάνει διατάξεις που ρυθμίζουν ζητήματα ευθύνης, γλωσσικού καθεστώτος, προστασίας δεδομένων προσωπικού χαρακτήρα (άρθρα 36-38), καθώς και κανόνες ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών και των ευαίσθητων, μη διαβαθμισμένων πληροφοριών (άρθρο 40). Περιγράφει τους κανόνες που διέπουν τη συνεργασία του Οργανισμού με τρίτες χώρες και διεθνείς οργανισμούς (άρθρο 39). Τέλος, και όχι λιγότερο σημαντικό, περιλαμβάνει διατάξεις σχετικά με την έδρα και τις συνθήκες λειτουργίας του Οργανισμού, καθώς και τον διοικητικό έλεγχο από τον Διαμεσολαβητή (άρθρα 41 και 42).

Ο τίτλος ΙΙΙ θεσπίζει το ευρωπαϊκό πλαίσιο πιστοποίησης της ασφάλειας στον κυβερνοχώρο (το «**πλαίσιο**») για τα προϊόντα και τις υπηρεσίες ΤΠΕ ως «lex generalis» (άρθρο 1). Καθορίζει τον γενικό σκοπό των ευρωπαϊκών συστημάτων ασφάλειας στον κυβερνοχώρο, δηλαδή τη διασφάλιση ότι τα προϊόντα και οι υπηρεσίες ΤΠΕ συμμορφώνονται με τις καθορισμένες απαιτήσεις σχετικά με την ασφάλεια στον κυβερνοχώρο όσον αφορά την ικανότητά τους να ανθίστανται, σε ένα δεδομένο επίπεδο εμπιστοσύνης, σε δράσεις που θέτουν σε κίνδυνο τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα των αποθηκευμένων, διαβιβασμένων ή επεξεργασμένων δεδομένων ή των σχετικών λειτουργιών ή υπηρεσιών (άρθρο 43). Επιπλέον, απαριθμεί τους στόχους ασφάλειας που επιδιώκουν τα ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο (άρθρο 45), όπως μεταξύ άλλων η ικανότητα προστασίας δεδομένων από τυχαία ή μη εξουσιοδοτημένη πρόσβαση ή κοινοποίηση, καταστροφή ή μετατροπή και το περιεχόμενο (δηλαδή τα στοιχεία) των ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο, όπως ο λεπτομερής καθορισμός του πεδίου εφαρμογής τους, των στόχων ασφάλειας, των κριτηρίων αξιολόγησης, κ.λπ. (άρθρο 47).

Ο τίτλος ΙΙΙ θεσπίζει επίσης τα κύρια έννομα αποτελέσματα των ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο, δηλαδή i) την υποχρέωση υλοποίησης του συστήματος σε εθνικό επίπεδο και τον εθελοντικό χαρακτήρα της πιστοποίησης· ii) την ακύρωση των εθνικών συστημάτων που αφορούν τα ίδια προϊόντα ή υπηρεσίες από τα ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στην κυβερνοχώρο (άρθρα 48 και 49).

Στον εν λόγω τίτλο καθορίζεται επίσης η διαδικασία για τη θέσπιση των ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο και οι αντίστοιχοι ρόλοι της Επιτροπής, του ENISA και της ευρωπαϊκής ομάδας πιστοποίησης της ασφάλειας στον κυβερνοχώρο - εφεξής η «Ομάδα» (άρθρο 44). Τέλος, στον τίτλο αυτό περιέχονται οι διατάξεις που διέπουν τους οργανισμούς αξιολόγησης της συμμόρφωσης, συμπεριλαμβανομένων των απαιτήσεων, των εξουσιών και των καθηκόντων τους, τις εθνικές εποπτικές αρχές πιστοποίησης, καθώς και κυρώσεις.

Η Ομάδα θεσπίζεται επίσης στον Τίτλο αυτό ως βασικός φορέας που αποτελείται από αντιπροσώπους εθνικών εποπτικών αρχών πιστοποίησης, των οποίων η κύρια λειτουργία είναι η συνεργασία με τον ENISA στην επεξεργασία ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο και η παροχή συμβουλών στην Επιτροπή σχετικά με γενικά ή ειδικά ζητήματα όσον αφορά την πολιτική πιστοποίησης της ασφάλειας στον κυβερνοχώρο.

Στον τίτλο IV του κανονισμού περιλαμβάνονται οι τελικές διατάξεις που περιγράφουν την άσκηση εξουσιοδότησης, τις απαιτήσεις αξιολόγησης, την κατάργηση και διαδοχή, καθώς και την έναρξη ισχύος.

2017/0225 (COD)

Πρόταση

ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

σχετικά με τον ENISA, τον «οργανισμό της ΕΕ για την ασφάλεια στον κυβερνοχώρο», και την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013, καθώς και σχετικά με την πιστοποίηση της ασφάλειας στον κυβερνοχώρο στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών («πράξη για την ασφάλεια στον κυβερνοχώρο»)

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ιδίως το άρθρο 114,

Έχοντας υπόψη την πρόταση της Ευρωπαϊκής Επιτροπής,

Κατόπιν διαβίβασης του σχεδίου νομοθετικής πράξης στα εθνικά κοινοβούλια,

Έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής[28],

Έχοντας υπόψη τη γνώμη της Επιτροπής των Περιφερειών[29],

Αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία,

Εκτιμώντας τα ακόλουθα:

(1) Τα συστήματα δικτύου και πληροφοριών και τα δίκτυα και οι υπηρεσίες τηλεπικοινωνιών διαδραματίζουν ζωτικό ρόλο για την κοινωνία και αποτελούν κεντρικό πυλώνα της οικονομικής ανάπτυξης. Η τεχνολογία πληροφοριών και επικοινωνιών ενισχύει τα σύνθετα συστήματα που στηρίζουν τις κοινωνικές δραστηριότητες, επιτρέπουν τη συνεχή λειτουργία των οικονομιών μας σε βασικούς τομείς όπως της υγείας, της ενέργειας, των οικονομικών και των μεταφορών, και στηρίζουν ειδικότερα τη λειτουργία της εσωτερικής αγοράς.

(2) Η χρήση συστημάτων δικτύου και πληροφοριών από τους πολίτες, τις επιχειρήσεις και τις κυβερνήσεις σε όλη την Ένωση είναι σήμερα ευρύτατα διαδεδομένη. Η ψηφιοποίηση και η συνδεσιμότητα καθίστανται πλέον βασικά χαρακτηριστικά στην περίπτωση ολοένα και περισσότερων προϊόντων και υπηρεσιών και με την έλευση του διαδικτύου των πραγμάτων, εκατομμύρια, αν όχι δισεκατομμύρια, συνδεδεμένες ψηφιακές συσκευές αναμένεται να χρησιμοποιούνται στην ΕΕ κατά την επόμενη δεκαετία. Αν και ολοένα μεγαλύτερος αριθμός συσκευών είναι συνδεδεμένες στο διαδίκτυο, η ασφάλεια και η ανθεκτικότητα δεν αποτελούν χαρακτηριστικά που

[28] ΕΕ C της , σ. .
[29] ΕΕ C της , σ. .

διαθέτουν επαρκώς από τον σχεδιασμό τους, με αποτέλεσμα την ανεπαρκή ασφάλειά τους στον κυβερνοχώρο. Στο πλαίσιο αυτό, η περιορισμένη χρήση της πιστοποίησης οδηγεί σε ανεπαρκείς πληροφορίες για τους χρήστες από οργανώσεις και τους μεμονωμένους χρήστες σχετικά με τα χαρακτηριστικά ασφάλειας στον κυβερνοχώρο των προϊόντων και των υπηρεσιών ΤΠΕ, με αποτέλεσμα την υπονόμευση της εμπιστοσύνης στις ψηφιακές λύσεις.

(3) Η αυξημένη ψηφιοποίηση και συνδεσιμότητα οδηγούν σε αυξημένους κινδύνους για την ασφάλεια στον κυβερνοχώρο, με αποτέλεσμα να καθίσταται η κοινωνία εν γένει πιο ευάλωτη σε απειλές τους κυβερνοχώρου και να οξύνονται οι κίνδυνοι που αντιμετωπίζουν τα φυσικά πρόσωπα, συμπεριλαμβανομένων των ευάλωτων προσώπων όπως τα παιδιά. Προκειμένου να μετριαστεί ο εν λόγω κίνδυνος για την κοινωνία, πρέπει να αναληφθούν όλες οι απαραίτητες ενέργειες για τη βελτίωση της ασφάλειας στον κυβερνοχώρο της ΕΕ με σκοπό την καλύτερη προστασία των συστημάτων δικτύου και πληροφοριών, των δικτύων τηλεπικοινωνιών, των ψηφιακών προϊόντων, υπηρεσιών και συσκευών που χρησιμοποιούν οι πολίτες, οι κυβερνήσεις και οι επιχειρήσεις – από τις ΜΜΕ έως τους διαχειριστές υποδομών ζωτικής σημασίας – από τις απειλές στον κυβερνοχώρο.

(4) Οι επιθέσεις στον κυβερνοχώρο παρουσιάζουν αύξηση και μια συνδεδεμένη οικονομία και κοινωνία που είναι πιο ευάλωτη σε απειλές και επιθέσεις στον κυβερνοχώρο χρειάζεται ισχυρότερη άμυνα. Ωστόσο, αν και οι επιθέσεις στον κυβερνοχώρο είναι συνήθως διασυνοριακές, τα πολιτικά μέτρα που λαμβάνουν οι αρχές για την ασφάλεια στον κυβερνοχώρο και οι αρμοδιότητες επιβολής του νόμου έχουν κυρίως εθνικό χαρακτήρα. Τα μεγάλης κλίμακας συμβάντα στον κυβερνοχώρο θα μπορούσαν να διαταράξουν την παροχή βασικών υπηρεσιών σε όλη την ΕΕ. Για να αντιμετωπιστούν οι επιθέσεις αυτές απαιτείται αποτελεσματική απόκριση και διαχείριση κρίσεων σε επίπεδο ΕΕ, με βάση ειδικές πολιτικές και ευρύτερα μέσα διασφάλισης της ευρωπαϊκής αλληλεγγύης και αμοιβαίας συνδρομής. Επιπλέον, η τακτική εκτίμηση της κατάστασης της ασφάλειας στον κυβερνοχώρο και της ανθεκτικότητας στην Ένωση με βάση αξιόπιστα ενωσιακά δεδομένα, καθώς και η συστηματική πρόβλεψη των μελλοντικών εξελίξεων, προκλήσεων και απειλών, τόσο σε ενωσιακό όσο και σε παγκόσμιο επίπεδο, είναι σημαντική για τους υπευθύνους χάραξης πολιτικής, τη βιομηχανία και τους χρήστες.

(5) Ενόψει των αυξημένων προκλήσεων που αντιμετωπίζει η Ένωση στον τομέα της ασφάλειας στον κυβερνοχώρο, υπάρχει ανάγκη για ολοκληρωμένη σειρά μέτρων που βασίζονται σε προηγούμενες δράσεις της Ένωσης και ευνοούν τους αλληλοενισχυόμενους στόχους. Σε αυτά περιλαμβάνεται η ανάγκη περαιτέρω αύξησης των ικανοτήτων και της ετοιμότητας των κρατών μελών και των επιχειρήσεων, καθώς και η ανάγκη βελτίωσης της συνεργασίας και του συντονισμού σε όλα τα κράτη μέλη και τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ. Επιπλέον, δεδομένης της διασυνοριακής φύσης των απειλών στον κυβερνοχώρο, υπάρχει ανάγκη αύξησης των ικανοτήτων σε επίπεδο Ένωσης που θα μπορούσαν να συμπληρώσουν τη δράση των κρατών μελών, ιδίως στην περίπτωση των μεγάλης κλίμακας διασυνοριακών συμβάντων και κρίσεων στον κυβερνοχώρο. Απαιτούνται επίσης επιπλέον προσπάθειες για την αύξηση της ευαισθητοποίησης των πολιτών και των επιχειρήσεων σε ζητήματα ασφάλειας στον κυβερνοχώρο. Επιπλέον, θα πρέπει να βελτιωθεί περαιτέρω η εμπιστοσύνη στην ψηφιακή ενιαία αγορά με την προσφορά διαφανών πληροφοριών σχετικά με το επίπεδο ασφάλειας των προϊόντων και των υπηρεσιών ΤΠΕ. Σε αυτό μπορεί να συμβάλει η πιστοποίηση σε επίπεδο ΕΕ, με την

παροχή κοινών απαιτήσεων ασφάλειας στον κυβερνοχώρο και κριτηρίων αξιολόγησης για όλες τις εθνικές αγορές και τους τομείς.

(6) Το 2004 το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο εξέδωσαν τον κανονισμό (ΕΚ) αριθ. 460/2004[30] για τη δημιουργία του ENISA με σκοπό να συμβάλλει στην επίτευξη των στόχων της διασφάλισης υψηλού επιπέδου ασφάλειας των δικτύων και των πληροφοριών εντός της Ένωσης και της ανάπτυξης μιας αντίληψης για την ασφάλεια των δικτύων και των πληροφοριών προς όφελος των πολιτών, των καταναλωτών, των επιχειρήσεων και των οργανισμών του δημόσιου τομέα. Το 2008 το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο εξέδωσαν τον κανονισμό (ΕΚ) αριθ. 1007/2008[31] για την παράταση της θητείας του Οργανισμού έως τον Μάρτιο του 2012. Ο κανονισμός (ΕΚ) αριθ. 580/2011[32] παρέτεινε περαιτέρω τη θητεία του Οργανισμού έως τις 13 Σεπτεμβρίου 2013. Το 2013 το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο εξέδωσαν τον κανονισμό (ΕΕ) αριθ. 526/2013[33] σχετικά με τον ENISA και την κατάργηση του κανονισμού (ΕΚ) αριθ. 460/2004, ο οποίος παρέτεινε τη θητεία του Οργανισμού έως τον Ιούνιο του 2020.

(7) Η Ένωση έχει λάβει ήδη σημαντικά μέτρα για τη διασφάλιση της ασφάλειας στον κυβερνοχώρο και την ενίσχυση της εμπιστοσύνης στις ψηφιακές τεχνολογίες. Το 2013 θεσπίστηκε Στρατηγική της ΕΕ για την ασφάλεια στον κυβερνοχώρο με σκοπό τον προσανατολισμό των μέτρων πολιτικής της Ένωσης έναντι των απειλών και των κινδύνων για την ασφάλεια στον κυβερνοχώρο. Στο πλαίσιο της προσπάθειάς της να προστατέψει καλύτερα τους Ευρωπαίους στο διαδίκτυο, η Ένωση θέσπισε το 2016 την πρώτη νομοθετική πράξη στον τομέα της ασφάλειας στον κυβερνοχώρο, την οδηγία (ΕΕ) 2016/1148 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (εφεξής η «οδηγία NIS»). Η οδηγία NIS θέσπισε απαιτήσεις σχετικά με τις ικανότητες σε εθνικό επίπεδο στον τομέα της ασφάλειας στον κυβερνοχώρο και τους πρώτους μηχανισμούς ενίσχυσης της στρατηγικής και επιχειρησιακής συνεργασίας μεταξύ των κρατών μελών και θέσπισε υποχρεώσεις όσον αφορά μέτρα ασφάλειας και κοινοποιήσεις συμβάντων σε διάφορους τομείς που είναι ζωτικής σημασίας για την οικονομία και την κοινωνία, όπως αυτοί της ενέργειας, των μεταφορών, της ύδρευσης, των τραπεζών, των υποδομών χρηματοπιστωτικών αγορών, της υγείας, της ψηφιακής υποδομής, καθώς και των βασικών παρόχων ψηφιακών υπηρεσιών (μηχανές αναζήτησης, υπηρεσίες νεφοϋπολογιστικής και επιγραμμικές αγορές). Στον ENISA ανατέθηκε κεντρικός ρόλος στην στήριξη της εφαρμογής της εν λόγω οδηγίας. Επιπλέον, σημαντική προτεραιότητα του ευρωπαϊκού θεματολογίου για την ασφάλεια

---

30 Κανονισμός (ΕΚ) αριθ. 460/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 10ης Μαρτίου 2004, για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια δικτύων και Πληροφοριών (ΕΕ L 77 της 13.3.2004, σ. 1).

31 Κανονισμός (ΕΚ) αριθ. 1007/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Σεπτεμβρίου 2008, περί τροποποιήσεως του κανονισμού (ΕΚ) αριθ. 460/2004 για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια δικτύων και Πληροφοριών ως προς τη διάρκειά του (ΕΕ L 293 της 31.10.2008, σ. 1).

32 Κανονισμός (ΕΕ) αριθ. 580/2011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 8ης Ιουνίου 2011, περί τροποποιήσεως του κανονισμού (ΕΚ) αριθ. 460/2004 για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια δικτύων και Πληροφοριών ως προς τη διάρκειά του (ΕΕ L 165 της 24.6.2011, σ. 3).

33 Κανονισμός (ΕΕ) αριθ. 526/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 21ης Μαΐου 2013, σχετικά με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) και την κατάργηση του κανονισμού (ΕΚ) αριθ. 460/2004 (ΕΕ L 165 της 18.6.2013, σ. 41).

είναι η αποτελεσματική καταπολέμηση του ηλεκτρονικού εγκλήματος, συμβάλλοντας έτσι στον συνολικό στόχο της επίτευξης υψηλού επιπέδου ασφάλειας στον κυβερνοχώρο.

(8) Αναγνωρίζεται ότι, από τη θέσπιση της Στρατηγικής της ΕΕ για την ασφάλεια στον κυβερνοχώρο το 2013 και την τελευταία επανεξέταση της εντολής του Οργανισμού, το συνολικό πολιτικό πλαίσιο έχει αλλάξει σημαντικά επίσης και σε σχέση με ένα πιο αβέβαιο και λιγότερο ασφαλές παγκόσμιο περιβάλλον. Σε συνάρτηση με τα παραπάνω και στο πλαίσιο της νέας πολιτικής της ΕΕ για την ασφάλεια στον κυβερνοχώρο, είναι απαραίτητο να επανεξεταστεί η εντολή του ENISA ώστε να καθοριστεί ο ρόλος του στο οικοσύστημα της ασφάλειας στον κυβερνοχώρο που έχει μεταβληθεί και να διασφαλιστεί η αποτελεσματική συμβολή του στην αντιμετώπιση από την Ένωση των προκλήσεων στον τομέα της ασφάλειας στον κυβερνοχώρο που απορρέουν από τη ριζική μεταβολή της φύσης των απειλών, οι οποίες, όπως αναγνωρίστηκε στο πλαίσιο της αξιολόγησης του Οργανισμού, δεν αντιμετωπίζονται επαρκώς από την παρούσα εντολή.

(9) Ο Οργανισμός που ιδρύεται με τον παρόντα κανονισμό θα πρέπει να αποτελεί συνέχεια του ENISA όπως συστάθηκε δυνάμει του κανονισμού (ΕΕ) αριθ. 526/2013. Ο Οργανισμός θα πρέπει να εκτελεί τα καθήκοντα που του ανατίθενται με τον παρόντα κανονισμό και τις νομοθετικές πράξεις της Ένωσης στον τομέα της ασφάλειας στον κυβερνοχώρο, μεταξύ άλλων, με την παροχή εμπειρογνωσίας και συμβουλών και μέσω της λειτουργίας του ως κέντρου πληροφοριών και γνώσεων της Ένωσης. Θα πρέπει να προωθεί την ανταλλαγή βέλτιστων πρακτικών μεταξύ των κρατών μελών και των άμεσα ενδιαφερόμενων του ιδιωτικού τομέα, με την υποβολή προτάσεων πολιτικής στην Ευρωπαϊκή Επιτροπή και τα κράτη μέλη, τη λειτουργία του ως σημείου αναφοράς για τομεακές πρωτοβουλίες πολιτικής της Ένωσης όσον αφορά ζητήματα ασφάλειας στον κυβερνοχώρο, την ενθάρρυνση της επιχειρησιακής συνεργασίας μεταξύ των κρατών μελών και μεταξύ των κρατών μελών και των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ.

(10) Με την απόφαση 2004/97/ΕΚ, Ευρατόμ που εκδόθηκε κατά τη σύνοδο του Ευρωπαϊκού Συμβουλίου της 13ης Δεκεμβρίου 2003, οι αντιπρόσωποι των κρατών μελών αποφάσισαν ότι ο ENISA θα είχε την έδρα του σε ελληνική πόλη που θα καθοριζόταν από την ελληνική κυβέρνηση. Το κράτος μέλος υποδοχής του Οργανισμού θα πρέπει να εξασφαλίζει τις βέλτιστες δυνατές συνθήκες για την εύρυθμη και αποδοτική λειτουργία του Οργανισμού. Για την απρόσκοπτη και αποτελεσματική εκτέλεση των καθηκόντων του, την πρόσληψη και τη διατήρηση προσωπικού, και την αύξηση της αποτελεσματικότητας της δράσης δικτύωσης, είναι αναγκαίο να έχει ο Οργανισμός τη βάση του σε κατάλληλο τόπο, που μεταξύ άλλων θα προσφέρει κατάλληλες μεταφορικές συνδέσεις και ευκολίες για τους συζύγους και τα τέκνα που θα συνοδεύουν το προσωπικό του Οργανισμού. Οι απαιτούμενες διευθετήσεις θα πρέπει να θεσπισθούν με συμφωνία μεταξύ του Οργανισμού και του κράτους μέλους υποδοχής, με προηγούμενη έγκριση του διοικητικού συμβουλίου του Οργανισμού.

(11) Δεδομένων των αυξανόμενων προκλήσεων που αντιμετωπίζει η Ένωση στον τομέα της ασφάλειας στον κυβερνοχώρο, θα πρέπει να αυξηθούν οι χρηματοδοτικοί και οι ανθρώπινοι πόροι του Οργανισμού, κατ' αντιστοιχία προς τον ενισχυμένο ρόλο και τα αυξημένα καθήκοντά του και την καθοριστική του θέση στο οικοσύστημα των οργανισμών που προασπίζονται το ευρωπαϊκό ψηφιακό οικοσύστημα.

(12) Ο Οργανισμός θα πρέπει, αφενός, να αναπτύσσει και να διατηρεί υψηλό επίπεδο εμπειρογνωσίας και, αφετέρου, να λειτουργεί ως σημείο αναφοράς, εμπνέοντας ασφάλεια και εμπιστοσύνη στην ενιαία αγορά χάρη στην ανεξαρτησία του, την ποιότητα των συμβουλών που παρέχει και των πληροφοριών που διαδίδει, τη διαφάνεια των διαδικασιών και μεθόδων λειτουργίας του και την επιμέλεια με την οποία εκτελεί τα καθήκοντά του. Ο Οργανισμός θα πρέπει να συμβάλλει προδραστικά στις εθνικές προσπάθειες και τις προσπάθειες σε επίπεδο Ένωσης και, παράλληλα, να εκτελεί τα καθήκοντά του σε στενή συνεργασία με τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και τα κράτη μέλη. Επιπροσθέτως, ο Οργανισμός θα πρέπει να αξιοποιεί τις εισροές από τον ιδιωτικό τομέα και άλλους σχετικούς άμεσα ενδιαφερομένους, καθώς και τη συνεργασία με αυτούς. Με μια σειρά καθηκόντων θα πρέπει να καθοριστεί ο τρόπος με τον οποίο Οργανισμός οφείλει να επιτύχει τους στόχους του, ενώ θα πρέπει να καθίσταται δυνατή η ευελιξία στο έργο του.

(13) Ο Οργανισμός θα πρέπει να επικουρεί την Επιτροπή μέσω συμβουλών, γνωμοδοτήσεων και αναλύσεων σχετικά με όλα τα θέματα της Ένωσης που αφορούν τη χάραξη, την επικαιροποίηση και την αναθεώρηση της πολιτικής και της νομοθεσίας στο πεδίο της ασφάλειας στον κυβερνοχώρο, περιλαμβανομένων της προστασίας των υποδομών ζωτικής σημασίας και της ανθεκτικότητας στον κυβερνοχώρο. Ο Οργανισμός θα πρέπει να ενεργεί ως σημείο αναφοράς σχετικά με τις συμβουλές και την εμπειρογνωσία για τομεακές πρωτοβουλίες πολιτικής και νομοθεσίας της Ένωσης σε περιπτώσεις που αφορούν ζητήματα ασφάλειας στην κυβερνοχώρο.

(14) Το βασικό καθήκον του Οργανισμού είναι η προώθηση της συνεπούς εφαρμογής του σχετικού νομικού πλαισίου, ιδίως της αποτελεσματικής εφαρμογής της οδηγίας NIS, που είναι απαραίτητη για την αύξηση της ανθεκτικότητας στον κυβερνοχώρο. Υπό το πρίσμα του ταχέως εξελισσόμενου τοπίου των απειλών για την ασφάλεια στον κυβερνοχώρο, είναι σαφές ότι θα πρέπει να παρέχεται στήριξη στα κράτη μέλη μέσω μιας πιο συνεκτικής διατομεακής προσέγγισης στην οικοδόμηση ανθεκτικότητας στον κυβερνοχώρο.

(15) Ο Οργανισμός θα πρέπει να επικουρεί τα κράτη μέλη και τα θεσμικά και λοιπά όργανα, υπηρεσίες και οργανισμούς της Ένωσης στην προσπάθειά τους να οικοδομήσουν και να ενισχύσουν τις ικανότητες και την ετοιμότητά τους για την πρόληψη, τον εντοπισμό και την αντιμετώπιση προβλημάτων και συμβάντων ασφάλειας στον κυβερνοχώρο και σε σχέση με την ασφάλεια συστημάτων δικτύου και πληροφοριών. Συγκεκριμένα, ο Οργανισμός θα πρέπει να υποστηρίζει την ανάπτυξη και την ενίσχυση εθνικών CSIRT, με σκοπό την επίτευξη υψηλού κοινού επιπέδου ωριμότητάς τους στην Ένωση. Ο Οργανισμός θα πρέπει επίσης να συμβάλλει στην ανάπτυξη και την επικαιροποίηση των στρατηγικών της Ένωσης και των κρατών μελών σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών, ιδίως όσον αφορά την ασφάλεια στον κυβερνοχώρο, να προωθεί τη διάδοσή τους και να παρακολουθεί την πρόοδο στην υλοποίησή τους. Ο Οργανισμός θα πρέπει επίσης να προσφέρει δυνατότητες κατάρτισης και εκπαιδευτικό υλικό στους δημόσιους φορείς και, όπου είναι σκόπιμο, να εκπαιδεύει τους εκπαιδευτικούς με σκοπό τη συνδρομή των κρατών μελών στην ανάπτυξη των δικών τους ικανοτήτων κατάρτισης.

(16) Ο Οργανισμός θα πρέπει να επικουρεί την ομάδα συνεργασίας που θεσπίστηκε με την οδηγία NIS στην εκτέλεση των καθηκόντων της, συγκεκριμένα μέσω της παροχής εμπειρογνωσίας, συμβουλών και της διευκόλυνσης της ανταλλαγής βέλτιστων πρακτικών, ιδίως όσον αφορά τον προσδιορισμό φορέων εκμετάλλευσης βασικών υπηρεσιών από τα κράτη μέλη, συμπεριλαμβανομένων μεταξύ άλλων όσον αφορά διασυνοριακές εξαρτήσεις σε σχέση με κινδύνους και συμβάντα.

(17) Με σκοπό την τόνωση της συνεργασίας μεταξύ του δημόσιου και του ιδιωτικού τομέα και εντός του ιδιωτικού τομέα και ειδικότερα με σκοπό τη στήριξη της προστασίας των υποδομών ζωτικής σημασίας, ο Οργανισμός θα πρέπει να διευκολύνει τη δημιουργία τομεακών κέντρων κοινοχρησίας και ανάλυσης πληροφοριών (ISAC) μέσω της παροχής βέλτιστων πρακτικών και καθοδήγησης όσον αφορά τα διαθέσιμα εργαλεία, τη διαδικασία, καθώς και με την παροχή καθοδήγησης για τον τρόπο αντιμετώπισης κανονιστικών ζητημάτων που σχετίζονται με την ανταλλαγή πληροφοριών.

(18) Ο Οργανισμός θα πρέπει να συγκεντρώνει και να αναλύει εθνικές εκθέσεις από CSIRT και τη CERT-EU και να καθορίζει κοινούς κανόνες, γλώσσα και ορολογία για την ανταλλαγή πληροφοριών. Ο Οργανισμός θα πρέπει επίσης να εξασφαλίζει τη συμμετοχή του ιδιωτικού τομέα, στο πλαίσιο της οδηγίας NIS που προβλέπει τους λόγους εθελούσιας ανταλλαγής τεχνικών πληροφοριών σε επιχειρησιακό επίπεδο με τη δημιουργία του δικτύου CSIRT.

(19) Ο Οργανισμός θα πρέπει να συμβάλλει στην αντιμετώπιση σε επίπεδο ΕΕ των μεγάλης κλίμακας διασυνοριακών συμβάντων και κρίσεων που αφορούν την ασφάλεια στον κυβερνοχώρο. Αυτή η λειτουργία θα πρέπει να περιλαμβάνει τη συλλογή σχετικών πληροφοριών και έναν διευκολυντικό ρόλο ανάμεσα στο δίκτυο CSIRT και στην τεχνική κοινότητα, καθώς και στους αρμόδιους λήψης αποφάσεων που είναι αρμόδιοι για τη διαχείριση κρίσεων. Επιπλέον, ο Οργανισμός θα μπορούσε να υποστηρίζει τον χειρισμό συμβάντων τεχνικής φύσης διευκολύνοντας τη σχετική τεχνική ανταλλαγή λύσεων μεταξύ των κρατών μελών και παρέχοντας εισροές σε δημόσιες επικοινωνίες. Ο Οργανισμός θα πρέπει να στηρίζει τη διαδικασία δοκιμάζοντας τις λεπτομέρειες μιας τέτοιας συνεργασίας μέσω ετήσιων ασκήσεων ασφάλειας στον κυβερνοχώρο.

(20) Για να εκπληρώνει τα επιχειρησιακά καθήκοντά του, ο Οργανισμός θα πρέπει να αξιοποιεί τη διαθέσιμη εμπειρογνωσία της CERT-EU μέσω διαρθρωμένης συνεργασίας, σε μικρή φυσική απόσταση. Η διαρθρωμένη συνεργασία θα διευκολύνει τις απαραίτητες συνέργειες και τη δημιουργία εμπειρογνωσίας του ENISA. Όπου συντρέχει περίπτωση, θα πρέπει να θεσπίζονται συγκεκριμένες ρυθμίσεις μεταξύ των δύο οργανισμών με σκοπό τον καθορισμό της πρακτικής εφαρμογής της εν λόγω συνεργασίας.

(21) Σε συμμόρφωση με τα επιχειρησιακά του καθήκοντα, ο Οργανισμός θα πρέπει να μπορεί να παρέχει στα κράτη μέλη στήριξη, π.χ. με την παροχή συμβουλών ή τεχνικής βοήθειας ή τη διασφάλιση αναλύσεων απειλών και συμβάντων. Σύμφωνα με τη σύσταση της Επιτροπής για τη συντονισμένη αντιμετώπιση συμβάντων και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο, τα κράτη μέλη πρέπει να συνεργάζονται με καλή πίστη και να ανταλλάσσουν μεταξύ τους και με τον ENISA, χωρίς αδικαιολόγητη καθυστέρηση, πληροφορίες σχετικά με μεγάλης κλίμακας συμβάντα και κρίσεις που αφορούν την ασφάλεια στον κυβερνοχώρο. Τέτοιου είδους πληροφορίες θα πρέπει να βοηθούν περαιτέρω τον ENISA στην εκπλήρωση των επιχειρησιακών καθηκόντων του.

(22) Στο πλαίσιο της τακτικής συνεργασίας σε τεχνικό επίπεδο με σκοπό τη στήριξη της ευαισθητοποίησης ως προς την κατάσταση στην Ένωση, ο Οργανισμός θα πρέπει να εκπονεί τακτικά την τεχνική έκθεση για την κατάσταση της ασφάλειας στον κυβερνοχώρο στην ΕΕ όσον αφορά συμβάντα και απειλές, με βάση τις πληροφορίες που είναι δημόσια διαθέσιμες, τις αναλύσεις του και εκθέσεις που έχει λάβει από τις CSIRT των κρατών μελών (σε εθελοντική βάση) ή ενιαία κέντρα επαφή της οδηγίας

NIS, το Ευρωπαϊκό Κέντρο για τα εγκλήματα στον κυβερνοχώρο (EC3) στη Europol, τη CERT-EU και, όπου συντρέχει περίπτωση, το Κέντρο ανάλυσης πληροφοριών της ΕΕ (INTCEN) στην Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης (ΕΥΕΔ). Η έκθεση θα πρέπει να διατίθεται στις αρμόδιες υπηρεσίες του Συμβουλίου, της Επιτροπής, τον Ύπατο Εκπρόσωπο της Ένωσης για Θέματα Εξωτερικής Πολιτικής και Πολιτικής Ασφαλείας και το δίκτυο CSIRT.

(23) Εκ των υστέρων τεχνικές έρευνες σχετικά με τα συμβάντα με σημαντικό αντίκτυπο σε περισσότερα από ένα κράτη μέλη, που έτυχαν υποστήριξης ή αναλήφθηκαν από τον Οργανισμό κατόπιν αιτήματος ή συναίνεσης του οικείου κράτους μέλους, θα πρέπει να εστιάζονται στην πρόληψη μελλοντικών συμβάντων και να διενεργούνται με την επιφύλαξη τυχόν δικαστικών ή διοικητικών διαδικασιών για την απόδοση ευθυνών ή τον καθορισμό υπαιτιότητας.

(24) Τα οικεία κράτη μέλη θα πρέπει να παρέχουν τις απαραίτητες πληροφορίες και συνδρομή στον Οργανισμό είτε για τους σκοπούς της έρευνας με την επιφύλαξη του άρθρου 346 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης είτε για άλλους λόγους δημόσιας τάξης.

(25) Τα κράτη μέλη μπορούν να καλούν τις επιχειρήσεις τις οποίες αφορά το συμβάν να συνεργάζονται παρέχοντας τις απαραίτητες πληροφορίες και συνδρομή στον Οργανισμό με την επιφύλαξη του δικαιώματός τους να προστατεύουν εμπορικά ευαίσθητες πληροφορίες.

(26) Για την καλύτερη κατανόηση των προκλήσεων στον τομέα της ασφάλειας στον κυβερνοχώρο και με σκοπό την παροχή στρατηγικών μακροπρόθεσμων συμβουλών στα κράτη μέλη και τα όργανα της Ένωσης, ο Οργανισμός πρέπει να αναλύει τους υφιστάμενους και αναδυόμενους κινδύνους. Για τον σκοπό αυτό, ο Οργανισμός θα πρέπει, σε συνεργασία με τα κράτη μέλη και, αν κρίνεται σκόπιμο, με τις στατιστικές υπηρεσίες και άλλους φορείς, να συλλέγει τις σχετικές πληροφορίες και να διενεργεί αναλύσεις των αναδυόμενων τεχνολογιών, καθώς και να παρέχει αξιολογήσεις για συγκεκριμένα θέματα σχετικά με τις αναμενόμενες κοινωνικές, νομικές, οικονομικές και ρυθμιστικές επιπτώσεις των τεχνολογικών καινοτομιών στην ασφάλεια δικτύων και πληροφοριών, και ειδικότερα στον κυβερνοχώρο. Ο Οργανισμός θα πρέπει επιπλέον να στηρίζει τα κράτη μέλη και τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης κατά τον προσδιορισμό των αναδυόμενων τάσεων και την πρόληψη των προβλημάτων που σχετίζονται με την ασφάλεια στον κυβερνοχώρο, πραγματοποιώντας αναλύσεις των απειλών και των συμβάντων.

(27) Προκειμένου να ενισχύσει την ανθεκτικότητα της Ένωσης, ο Οργανισμός θα πρέπει να αναπτύσσει αριστεία σχετικά με το αντικείμενο της ασφάλειας της υποδομής του διαδικτύου και των κρίσιμων υποδομών, παρέχοντες συμβουλές, καθοδήγηση και βέλτιστες πρακτικές. Με στόχο τη διασφάλιση ευκολότερης πρόσβασης σε καλύτερα διαρθρωμένες πληροφορίες σχετικά με τους κινδύνους και τα ενδεχόμενα διορθωτικά μέτρα που αφορούν την ασφάλεια στον κυβερνοχώρο, ο Οργανισμός θα πρέπει να αναπτύξει και να διατηρεί τον «κόμβο πληροφοριών» της Ένωσης, μια μονοαπευθυντική πύλη που παρέχει στο κοινό πληροφορίες σχετικά με την ασφάλεια στον κυβερνοχώρο προερχόμενες από τα θεσμικά και λοιπά όργανα και τους οργανισμούς σε επίπεδο ΕΕ και κρατών μελών.

(28) Ο Οργανισμός θα πρέπει να συμβάλλει στην ευαισθητοποίηση του κοινού σχετικά με τους κινδύνους που σχετίζονται με την ασφάλεια στον κυβερνοχώρο και να παρέχει καθοδήγηση όσον αφορά τις ορθές πρακτικές για μεμονωμένους χρήστες στοχεύοντας σε πολίτες και οργανώσεις. Ο Οργανισμός θα πρέπει επίσης να συμβάλλει στην

προώθηση βέλτιστων πρακτικών και λύσεων σε επίπεδο ατόμων και οργανώσεων, συλλέγοντας και αναλύοντας δημόσια διαθέσιμες πληροφορίες σχετικά με σημαντικά συμβάντα, και συντάσσοντας εκθέσεις, με σκοπό αφενός την παροχή καθοδήγησης σε επιχειρήσεις και πολίτες και αφετέρου τη βελτίωση του συνολικού επιπέδου ετοιμότητας και ανθεκτικότητας. Επιπλέον, ο Οργανισμός θα πρέπει να διοργανώνει, σε συνεργασία με τα κράτη μέλη και τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης, τακτικές εκστρατείες προβολής και ενημέρωσης του κοινού που θα απευθύνονται στους τελικούς χρήστες, με στόχο την προώθηση ασφαλέστερων ατομικών συμπεριφορών στον κυβερνοχώρο και την ευαισθητοποίηση σχετικά με τις πιθανές απειλές στον κυβερνοχώρο, συμπεριλαμβανομένων ηλεκτρονικών εγκλημάτων, όπως επιθέσεις ηλεκτρονικού «ψαρέματος» (phishing), τα δίκτυα υπολογιστών που έχουν προσβληθεί από προγράμματα ρομπότ (botnet), η χρηματοπιστωτική και τραπεζική απάτη, καθώς και με βασικές συμβουλές για την πιστοποίηση γνησιότητας και την προστασία των δεδομένων. Ο Οργανισμός θα πρέπει να διαδραματίζει κεντρικό ρόλο στην επιτάχυνση της ευαισθητοποίησης των τελικών χρηστών ως προς την ασφάλεια των συσκευών.

(29) Προκειμένου να υποστηρίζει τις επιχειρήσεις που δραστηριοποιούνται στον τομέα της ασφάλειας στον κυβερνοχώρο, καθώς και τους χρήστες λύσεων σχετικών με την ασφάλεια στον κυβερνοχώρο, ο Οργανισμός θα πρέπει να αναπτύξει και να διατηρεί ένα «παρατηρητήριο αγοράς», διενεργώντας τακτικές αναλύσεις και μεριμνώντας για τη διάδοση των κύριων τάσεων στην αγορά της ασφάλειας στον κυβερνοχώρο, τόσο από την πλευρά της ζήτησης όσο και από την πλευρά της προσφοράς.

(30) Για να διασφαλίσει την πλήρη επιτυχία των στόχων του, ο Οργανισμός θα πρέπει να συνεργάζεται με σχετικά όργανα, οργανισμούς και υπηρεσίες, όπως είναι η CERT-EU, το Ευρωπαϊκό Κέντρο για τα Εγκλήματα στον Κυβερνοχώρο (EC3) στο πλαίσιο της Ευρωπόλ, ο Ευρωπαϊκός Οργανισμός για τη λειτουργική διαχείριση συστημάτων ΤΠ μεγάλης κλίμακας (eu-LISA), ο Ευρωπαϊκός Οργανισμός Ασφάλειας της Αεροπορίας (EOAA) και κάθε άλλος οργανισμός της ΕΕ που εμπλέκεται στην ασφάλεια στον κυβερνοχώρο. Ο Οργανισμός θα πρέπει επίσης να συνεργάζεται με αρχές που ασχολούνται με την προστασία των δεδομένων, προκειμένου να ανταλλάσσει τεχνογνωσία και βέλτιστες πρακτικές και να παρέχει συμβουλές σε πτυχές της ασφάλειας στον κυβερνοχώρο που ενδέχεται να έχουν επιπτώσεις στο έργο τους. Οι εκπρόσωποι των εθνικών και των ενωσιακών αρχών επιβολής του νόμου και προστασίας δεδομένων θα πρέπει να έχουν δικαίωμα εκπροσώπησης στη μόνιμη ομάδα ενδιαφερομένων του Οργανισμού. Όταν ο Οργανισμός συνεργάζεται με φορείς επιβολής του νόμου για θέματα ασφάλειας των δικτύων και των πληροφοριών τα οποία ενδέχεται να έχουν επιπτώσεις στο έργο τους, θα πρέπει να σέβεται τους υπάρχοντες διαύλους πληροφοριών και τα υφιστάμενα δίκτυα.

(31) Ο Οργανισμός, ως μέλος που παρέχει επιπλέον γραμματειακή υποστήριξη στο δίκτυο CSIRT, θα πρέπει να στηρίζει τις CSIRT των κρατών μελών και τη CERT-EU στην επιχειρησιακή συνεργασία πέραν όλων των σχετικών καθηκόντων του δικτύου CSIRT, όπως προβλέπει η οδηγία για την ασφάλεια δικτύων και πληροφοριών. Ακόμη, ο Οργανισμός θα πρέπει να προωθεί και να υποστηρίζει τη συνεργασία μεταξύ των οικείων CSIRT σε περίπτωση περιστατικών, επιθέσεων ή διαταραχών στη λειτουργία των δικτύων ή στην υποδομή την οποία διαχειρίζονται ή προστατεύουν οι CSIRT και αφορούν ή μπορεί να αφορούν τουλάχιστον δύο CSIRT, λαμβάνοντας δεόντως υπόψη τις τυποποιημένες επιχειρησιακές διαδικασίες του δικτύου CSIRT.

(32) Προκειμένου να αυξηθεί η ετοιμότητα της Ένωσης στην απόκριση σε συμβάντα ασφάλειας στον κυβερνοχώρο, ο Οργανισμός θα πρέπει να οργανώνει σε ετήσια βάση

ασκήσεις για την ασφάλεια στον κυβερνοχώρο σε επίπεδο Ένωσης και, κατόπιν αιτήματος, να στηρίζει τα κράτη μέλη και τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ στην οργάνωση ασκήσεων.

(33) Ο Οργανισμός θα πρέπει να αναπτύσσει περαιτέρω και να διατηρεί την εμπειρογνωσία του στην πιστοποίηση της ασφάλειας στον κυβερνοχώρο προκειμένου να υποστηρίζει την ενωσιακή πολιτική στον τομέα αυτό. Ο Οργανισμός θα πρέπει να προάγει την εισαγωγή πιστοποίησης για την ασφάλεια στον κυβερνοχώρο εντός της Ένωσης, μεταξύ άλλων συμβάλλοντας στη θέσπιση και τη διατήρηση ενός πλαισίου πιστοποίησης της ασφάλειας στον κυβερνοχώρο σε ενωσιακό επίπεδο, προκειμένου να αυξηθεί η διαφάνεια της διασφάλισης της ασφάλειας στον κυβερνοχώρο για προϊόντα και υπηρεσίες ΤΠΕ και, επομένως, να ενισχυθεί η εμπιστοσύνη στην ψηφιακή εσωτερική αγορά.

(34) Οι αποδοτικές πολιτικές ασφάλειας στον κυβερνοχώρο θα πρέπει να βασίζονται σε σωστά εκπονηθείσες μεθόδους εκτίμησης κινδύνου, τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα. Οι μέθοδοι εκτίμησης κινδύνου χρησιμοποιούνται σε διαφορετικά επίπεδα και δεν υπάρχουν κοινές πρακτικές όσον αφορά την αποδοτική εφαρμογή τους. Η προώθηση και ανάπτυξη βέλτιστων πρακτικών για την εκτίμηση κινδύνου και για διαλειτουργικές λύσεις διαχείρισης κινδύνου σε οργανισμούς του δημοσίου και του ιδιωτικού τομέα θα βελτιώσει το επίπεδο ασφάλειας στον κυβερνοχώρο στην Ένωση. Για τον σκοπό αυτό, ο Οργανισμός θα πρέπει να υποστηρίζει τη συνεργασία μεταξύ των ενδιαφερομένων του δημόσιου και του ιδιωτικού τομέα σε επίπεδο Ένωσης, διευκολύνοντας τις προσπάθειές τους σχετικά με την καθιέρωση και χρήση ευρωπαϊκών και διεθνών προτύπων για τη διαχείριση κινδύνου και τη μετρήσιμη ασφάλεια ηλεκτρονικών προϊόντων, συστημάτων, δικτύων και υπηρεσιών που, μαζί με το λογισμικό, αποτελούν τα συστήματα δικτύων και πληροφοριών.

(35) Ο Οργανισμός θα πρέπει να παροτρύνει τα κράτη μέλη και τους παρόχους υπηρεσιών να ανεβάζουν το γενικό επίπεδο των προτύπων ασφαλείας, έτσι ώστε όλοι οι χρήστες του διαδικτύου να μπορούν να λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίζουν την προσωπική τους ασφάλεια στον κυβερνοχώρο. Πιο συγκεκριμένα, οι πάροχοι υπηρεσιών και οι κατασκευαστές προϊόντων θα πρέπει να αποσύρουν ή να ανακυκλώνουν προϊόντα και υπηρεσίες που δεν πληρούν τα πρότυπα ασφάλειας στον κυβερνοχώρο. Σε συνεργασία με τις αρμόδιες αρχές, ο ENISA μπορεί να διαδίδει πληροφορίες όσον αφορά το επίπεδο ασφάλειας στον κυβερνοχώρο των προϊόντων και των υπηρεσιών που διατίθενται στην εσωτερική αγορά και να εκδίδει προειδοποιήσεις που στοχεύουν τους παρόχους και τους κατασκευαστές και απαιτούν από αυτούς να βελτιώνουν την ασφάλεια, συμπεριλαμβανομένης της ασφάλειας στον κυβερνοχώρο, των προϊόντων και των υπηρεσιών τους.

(36) Ο Οργανισμός θα πρέπει να λαμβάνει πλήρως υπόψη τις τρέχουσες δραστηριότητες έρευνας, ανάπτυξης και τεχνικής αξιολόγησης, ιδίως εκείνες που πραγματοποιούνται στο πλαίσιο διαφόρων ερευνητικών πρωτοβουλιών της Ένωσης, προκειμένου να συμβουλεύει τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και, όπου είναι σκόπιμο, τα κράτη μέλη, εφόσον το ζητήσουν, σχετικά με τις ερευνητικές ανάγκες στον τομέα της ασφάλειας των δικτύων και πληροφοριών και ιδίως της ασφάλειας στον κυβερνοχώρο.

(37) Τα προβλήματα ασφάλειας στον κυβερνοχώρο είναι παγκόσμια. Υπάρχει ανάγκη στενότερης διεθνούς συνεργασίας για τη βελτίωση των προτύπων ασφαλείας, συμπεριλαμβανομένων του ορισμού κοινών προτύπων συμπεριφοράς και της από κοινού χρήσης πληροφοριών, η οποία να προωθεί μια ταχύτερη διεθνή συνεργασία σε

θέματα απόκρισης καθώς και κοινή παγκόσμια προσέγγιση των θεμάτων ασφάλειας δικτύων και πληροφοριών. Για τον σκοπό αυτό ο Οργανισμός θα πρέπει να υποστηρίζει την εκτενέστερη ενωσιακή συμμετοχή και τη συνεργασία με τρίτες χώρες και διεθνείς οργανισμούς, παρέχοντας, αν κρίνεται σκόπιμο, την απαιτούμενη εμπειρογνωσία και δυνατότητα ανάλυσης στα σχετικά θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης.

(38) Ο Οργανισμός θα πρέπει να είναι ικανός να ανταποκρίνεται σε ad hoc αιτήματα παροχής συμβουλών και επικουρίας που υποβάλλουν τα κράτη μέλη και τα θεσμικά και λοιπά όργανα και οι οργανισμοί της ΕΕ και εμπίπτουν στους στόχους του Οργανισμού.

(39) Είναι αναγκαίο να εφαρμοστούν ορισμένες αρχές σε σχέση με τη διακυβέρνηση του Οργανισμού, προκειμένου να συμμορφώνεται προς την κοινή δήλωση και την κοινή προσέγγιση που συμφωνήθηκαν τον Ιούλιο του 2012 στη διοργανική ομάδα εργασίας για τους αποκεντρωμένους οργανισμούς της ΕΕ, η οποία κοινή δήλωση και προσέγγιση έχει ως αποστολή τον εξορθολογισμό των δραστηριοτήτων των οργανισμών και τη βελτίωση της απόδοσής τους. Η κοινή δήλωση και η κοινή προσέγγιση θα πρέπει επίσης να αντικατοπτρίζονται κατάλληλα στα προγράμματα εργασιών του Οργανισμού, στις αξιολογήσεις του, και στις πρακτικές του όσον αφορά την υποβολή εκθέσεων και την άσκηση της διοίκησης.

(40) Το διοικητικό συμβούλιο, που απαρτίζεται από τα κράτη μέλη και την Επιτροπή, θα πρέπει να καθορίζει τη γενική κατεύθυνση των εργασιών του Οργανισμού και να διασφαλίζει ότι ο Οργανισμός εκτελεί τα καθήκοντά του σύμφωνα με τον παρόντα κανονισμό. Θα πρέπει να εκχωρηθούν στο διοικητικό συμβούλιο οι αναγκαίες εξουσίες για την κατάρτιση του προϋπολογισμού, τον έλεγχο της εκτέλεσής του, την έγκριση κατάλληλων δημοσιονομικών κανόνων, τη θέσπιση διαφανών διαδικασιών εργασίας για τη λήψη αποφάσεων από τον Οργανισμό, την έγκριση του ενιαίου εγγράφου προγραμματισμού του Οργανισμού, την έγκριση του εσωτερικού κανονισμού του Οργανισμού, καθώς και τον διορισμό του εκτελεστικού διευθυντή και τη λήψη απόφασης για παράταση της θητείας του εκτελεστικού διευθυντή καθώς και για τη λήξη της.

(41) Για την ορθή και αποτελεσματική λειτουργία του Οργανισμού, η Επιτροπή και τα κράτη μέλη θα πρέπει να εξασφαλίζουν ότι τα πρόσωπα που θα διορισθούν στο διοικητικό συμβούλιο έχουν την κατάλληλη επαγγελματική εμπειρογνωσία και πείρα σε λειτουργικούς τομείς. Η Επιτροπή και τα κράτη μέλη θα πρέπει επίσης να καταβάλλουν προσπάθειες για τον περιορισμό της εναλλαγής των αντίστοιχων εκπροσώπων τους στο διοικητικό συμβούλιο, προκειμένου να εξασφαλίζεται η συνέχεια του έργου του.

(42) Για την ομαλή λειτουργία του Οργανισμού, ο εκτελεστικός διευθυντής του επιβάλλεται να διορίζεται βάσει προσόντων και αποδεδειγμένων διοικητικών και διευθυντικών ικανοτήτων, καθώς και βάσει ικανοτήτων και πείρας στον τομέα της ασφάλειας στον κυβερνοχώρο, και να εκτελεί τα καθήκοντά του εκτελεστικού διευθυντή σε πλήρη ανεξαρτησία. Ο εκτελεστικός διευθυντής θα πρέπει να εκπονεί πρόταση για το πρόγραμμα εργασίας του Οργανισμού, κατόπιν προηγούμενης διαβούλευσης με την Επιτροπή, και να λαμβάνει όλα τα αναγκαία μέτρα για να διασφαλίζει την ορθή εκτέλεση του προγράμματος εργασίας του Οργανισμού. Ο εκτελεστικός διευθυντής θα πρέπει να καταρτίζει ετήσια έκθεση και να την υποβάλλει στο διοικητικό συμβούλιο, να εκπονεί σχέδιο κατάστασης των προβλεπόμενων εσόδων και εξόδων του Οργανισμού, και να εκτελεί τον προϋπολογισμό. Επιπλέον, ο

εκτελεστικός διευθυντής θα πρέπει να έχει τη δυνατότητα να συγκροτεί ad hoc ομάδες εργασίας για την αντιμετώπιση ειδικών θεμάτων, ειδικότερα επιστημονικής, τεχνικής, νομικής ή κοινωνικοοικονομικής φύσης. Ο εκτελεστικός διευθυντής θα πρέπει να διασφαλίζει ότι τα μέλη των ad hoc ομάδων εργασίας επιλέγονται σύμφωνα με τα υψηλότερα πρότυπα εμπειρογνωσίας, λαμβάνοντας δεόντως υπόψη μια ισορροπημένη εκπροσώπηση, όπου κρίνεται σκόπιμο αναλόγως του συγκεκριμένου θέματος προς συζήτηση, των δημόσιων διοικήσεων των κρατών μελών, των θεσμικών οργάνων της Ένωσης και του ιδιωτικού τομέα, συμπεριλαμβανομένου του επιχειρηματικού κλάδου, των χρηστών και των πανεπιστημιακών που είναι ειδικοί στο πεδίο της ασφάλειας δικτύων και πληροφοριών.

(43) Το εκτελεστικό συμβούλιο θα πρέπει να συμβάλλει στην αποτελεσματική λειτουργία του διοικητικού συμβουλίου. Στο πλαίσιο των προπαρασκευαστικών εργασιών του που σχετίζονται με τις αποφάσεις του διοικητικού συμβουλίου, το εκτελεστικό συμβούλιο θα πρέπει να εξετάζει λεπτομερώς τις σχετικές πληροφορίες, να διερευνά τις διαθέσιμες επιλογές και να παρέχει συμβουλές και λύσεις για την εκπόνηση σχετικών αποφάσεων του διοικητικού συμβουλίου.

(44) Ο Οργανισμός θα πρέπει να διαθέτει μια μόνιμη ομάδα ενδιαφερομένων ως συμβουλευτικό όργανο, προκειμένου να διασφαλίζει τον τακτικό διάλογο με τον ιδιωτικό τομέα, τις οργανώσεις καταναλωτών και άλλους σχετικούς άμεσα ενδιαφερομένους. Η μόνιμη ομάδα ενδιαφερομένων, η οποία συγκροτείται από το διοικητικό συμβούλιο κατόπιν πρότασης του εκτελεστικού διευθυντή, θα πρέπει να επικεντρώνεται σε θέματα που αφορούν τους άμεσα ενδιαφερομένους και να τα θέτει υπόψη του Οργανισμού. Η σύνθεση της μόνιμης ομάδας ενδιαφερομένων και τα καθήκοντα με τα οποία επιφορτίζεται αυτή η ομάδα, η γνώμη της οποίας ζητείται ιδίως όσον αφορά το σχέδιο προγράμματος εργασίας, θα πρέπει να διασφαλίζουν επαρκή αντιπροσώπευση των ενδιαφερομένων στις εργασίες του Οργανισμού.

(45) Ο Οργανισμός θα πρέπει να θεσπίσει και να εφαρμόζει κανόνες για την πρόληψη και τη διαχείριση συγκρούσεων συμφερόντων. Ο Οργανισμός θα πρέπει επίσης να εφαρμόζει τη σχετική νομοθεσία της Ένωσης για την πρόσβαση του κοινού σε έγγραφα κατά τα οριζόμενα στον κανονισμό (ΕΚ) αριθ. 1049/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[34]. Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα από τον Οργανισμό θα πρέπει να υπόκειται στον κανονισμό (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Δεκεμβρίου 2000, σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών[35]. Ο Οργανισμός θα πρέπει να συμμορφώνεται με τις διατάξεις που ισχύουν για τα θεσμικά όργανα της Ένωσης, καθώς και με την εθνική νομοθεσία σχετικά με τον χειρισμό πληροφοριών, ιδίως των ευαίσθητων μη διαβαθμισμένων πληροφοριών και των διαβαθμισμένων πληροφοριών της ΕΕ.

(46) Προκειμένου να διασφαλισθεί η πλήρης αυτονομία και ανεξαρτησία του Οργανισμού και για να είναι σε θέση ο Οργανισμός να ασκήσει πρόσθετα και νέα καθήκοντα, ακόμα κι αν αυτά είναι έκτακτα και απρόβλεπτα, θα πρέπει να διατεθεί στον

---

34 Κανονισμός (ΕΚ) αριθ. 1049/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 30ής Μαΐου 2001, για την πρόσβαση του κοινού στα έγγραφα του Ευρωπαϊκού Κοινοβουλίου, του Συμβουλίου και της Επιτροπής (ΕΕ L 145 της 31.5.2001, σ. 43).

35 ΕΕ L 8 της 12.1.2001, σ. 1.

Οργανισμό επαρκής και αυτόνομος προϋπολογισμός του οποίου τα έσοδα να προέρχονται πρωτίστως από εισφορές της Ένωσης και από εισφορές τρίτων χωρών που συμμετέχουν στις εργασίες του Οργανισμού. Η πλειονότητα των υπαλλήλων του Οργανισμού θα πρέπει να εμπλέκεται άμεσα στην επιτέλεση των επιχειρησιακών καθηκόντων στο πλαίσιο της εντολής του Οργανισμού. Θα πρέπει να επιτρέπεται στο κράτος μέλος υποδοχής ή σε οποιοδήποτε άλλο κράτος μέλος να συνεισφέρει εθελοντικά στα έσοδα του Οργανισμού. Η δημοσιονομική διαδικασία της Ένωσης θα πρέπει να παραμένει σε ισχύ όσον αφορά τις επιδοτήσεις που βαρύνουν τον γενικό προϋπολογισμό της Ένωσης. Επιπλέον, το Ευρωπαϊκό Ελεγκτικό Συνέδριο θα πρέπει να προβαίνει σε έλεγχο των λογαριασμών για να εξασφαλίζει διαφάνεια και λογοδοσία.

(47) Αξιολόγηση της συμμόρφωσης είναι η διαδικασία με την οποία αποδεικνύεται κατά πόσο πληρούνται οι ειδικές απαιτήσεις που αφορούν προϊόν, διαδικασία, υπηρεσία, σύστημα, πρόσωπο ή φορέα. Για τους σκοπούς του παρόντος κανονισμού, η πιστοποίηση θα πρέπει να θεωρείται ως ένα είδος αξιολόγησης της συμμόρφωσης, ως προς τα χαρακτηριστικά της ασφάλειας στον κυβερνοχώρο, ενός προϊόντος, μιας διαδικασίας, μιας υπηρεσίας, ενός συστήματος ή συνδυασμού αυτών («προϊόντα και υπηρεσίες ΤΠΕ») από ανεξάρτητο τρίτο μέρος, άλλο από τον κατασκευαστή του προϊόντος ή τον πάροχο της υπηρεσίας. Η πιστοποίηση δεν μπορεί να εγγυηθεί αυτή καθαυτή ότι τα προϊόντα και οι υπηρεσίες ΤΠΕ που έχουν λάβει πιστοποίηση είναι ασφαλή στον κυβερνοχώρο. Πρόκειται μάλλον για μια διαδικασία και μια τεχνική μεθοδολογία που βεβαιώνει ότι τα προϊόντα και οι υπηρεσίες ΤΠΕ έχουν δοκιμαστεί και ότι συμμορφώνονται με ορισμένες απαιτήσεις ασφάλειας στον κυβερνοχώρο που προβλέπονται αλλού, για παράδειγμα όπως καθορίζονται σε τεχνικά πρότυπα.

(48) Η πιστοποίηση της ασφάλειας στον κυβερνοχώρο παίζει σημαντικό ρόλο στην ενίσχυση της αξιοπιστίας και της ασφάλειας για τα προϊόντα και τις υπηρεσίες ΤΠΕ. Η ψηφιακή ενιαία αγορά, και πιο συγκεκριμένα η οικονομία δεδομένων και το διαδίκτυο των πραγμάτων, μπορούν να ευδοκιμήσουν μόνο αν υπάρχει εμπιστοσύνη από το ευρύ κοινό ότι αυτά τα προϊόντα και αυτές οι υπηρεσίες παρέχουν ένα ορισμένο επίπεδο διασφάλισης της ασφάλειας στον κυβερνοχώρο. Τα συνδεδεμένα και αυτοματοποιημένα αυτοκίνητα, οι ηλεκτρονικές ιατρικές συσκευές, τα συστήματα ελέγχου βιομηχανικού αυτοματισμού ή τα ευφυή δίκτυα είναι μόνο μερικά παραδείγματα τομέων όπου η πιστοποίηση χρησιμοποιείται ήδη ευρέως ή ενδέχεται να χρησιμοποιηθεί στο εγγύς μέλλον. Οι τομείς που ρυθμίζονται από την οδηγία για την ασφάλεια δικτύων και πληροφοριών είναι επίσης τομείς στους οποίους η πιστοποίηση της ασφάλειας στον κυβερνοχώρο είναι καίριας σημασίας.

(49) Στην ανακοίνωση που εξέδωσε το 2016 με τίτλο «Ενίσχυση του συστήματος κυβερνοανθεκτικότητας της Ευρώπης και προώθηση ανταγωνιστικού και καινοτόμου κλάδου ασφάλειας στον κυβερνοχώρο», η Επιτροπή επισήμανε την ανάγκη για υψηλής ποιότητας, οικονομικά και διαλειτουργικά προϊόντα και λύσεις για την ασφάλεια στον κυβερνοχώρο. Η προμήθεια προϊόντων και υπηρεσιών ΤΠΕ εντός της ενιαίας αγοράς παραμένει πολύ κατακερματισμένη γεωγραφικά. Αυτό οφείλεται στο γεγονός ότι ο κλάδος της ασφάλειας στον κυβερνοχώρο στην Ευρώπη έχει αναπτυχθεί στο παρελθόν σε μεγάλο βαθμό με βάση τη ζήτηση από τις εθνικές κυβερνήσεις. Επιπλέον, η έλλειψη διαλειτουργικών λύσεων (τεχνικών προτύπων), πρακτικών και μηχανισμών πιστοποίησης σε επίπεδο ΕΕ συμπεριλαμβάνεται στα λοιπά κενά που επηρεάζουν την ενιαία αγορά στον τομέα της ασφάλειας στον κυβερνοχώρο. Αφενός, το γεγονός αυτό καθιστά δύσκολο τον ανταγωνισμό μεταξύ των ευρωπαϊκών εταιρειών σε εθνικό, ευρωπαϊκό και παγκόσμιο επίπεδο και, αφετέρου, μειώνει την

επιλογή βιώσιμων και χρήσιμων τεχνολογιών ασφάλειας στον κυβερνοχώρο στις οποίες έχουν πρόσβαση τα φυσικά πρόσωπα και οι επιχειρήσεις. Ομοίως, στην ενδιάμεση επανεξέταση της εφαρμογής της στρατηγικής για την ψηφιακή ενιαία αγορά, η Επιτροπή επισήμανε την ανάγκη για ασφαλή συνδεδεμένα προϊόντα και συστήματα και ανέφερε ότι η δημιουργία ενός ευρωπαϊκού πλαισίου ασφάλειας ΤΠΕ βάσει του οποίου θεσπίζονται κανόνες για τον τρόπο οργάνωσης της πιστοποίησης ασφάλειας ΤΠΕ στην Ένωση μπορεί να διαφυλάξει την εμπιστοσύνη στο διαδίκτυο, καθώς και να αντιμετωπίσει τον υφιστάμενο κατακερματισμό της αγοράς ασφάλειας στον κυβερνοχώρο.

(50) Επί του παρόντος, η πιστοποίηση της ασφάλειας στον κυβερνοχώρο για τα προϊόντα και τις υπηρεσίες ΤΠΕ χρησιμοποιείται μόνο σε περιορισμένη κλίμακα. Όπου υπάρχει, πρόκειται κυρίως για χρήση σε επίπεδο κράτους μέλους ή στο πλαίσιο συστημάτων κατευθυνόμενων από τη βιομηχανία. Στο πλαίσιο αυτό, ένα πιστοποιητικό που εκδίδεται από μια εθνική αρχή ασφάλειας στον κυβερνοχώρο δεν αναγνωρίζεται καταρχήν από τα άλλα κράτη μέλη. Επομένως, οι εταιρείες πρέπει να πιστοποιούν τα προϊόντα και τις υπηρεσίες τους στα κράτη μέλη όπου δραστηριοποιούνται, για παράδειγμα με σκοπό τη συμμετοχή τους σε εθνικές διαδικασίες προμηθειών. Επιπλέον, ενώ νέα συστήματα κάνουν την εμφάνισή τους, δεν φαίνεται να υπάρχει συνεκτική και ολιστική προσέγγιση όσον αφορά τα οριζόντια ζητήματα ασφάλειας στον κυβερνοχώρο, για παράδειγμα στο πεδίο του διαδικτύου των πραγμάτων. Τα υφιστάμενα συστήματα παρουσιάζουν σοβαρές αδυναμίες και διαφορές ως προς την κάλυψη των προϊόντων, τα επίπεδα διασφάλισης, τα ουσιαστικά κριτήρια και την πραγματική χρήση.

(51) Στο παρελθόν έχουν καταβληθεί προσπάθειες προκειμένου να επιτευχθεί μια αμοιβαία αναγνώριση πιστοποιητικών στην Ευρώπη. Ωστόσο, οι προσπάθειες δεν στέφτηκαν με πλήρη επιτυχία. Το πιο αξιοσημείωτο παράδειγμα προς αυτήν την κατεύθυνση είναι η συμφωνία αμοιβαίας αναγνώρισης (MRA) της Ομάδας Ανώτερων Υπαλλήλων για την Ασφάλεια των Συστημάτων Πληροφοριών (SOG-IS). Παρότι αντιπροσωπεύει το πιο σημαντικό μοντέλο συνεργασίας και αμοιβαίας αναγνώρισης στο πεδίο της πιστοποίησης της ασφάλειας, η συμφωνία αμοιβαίας αναγνώρισης της SOG-IS παρουσιάζει σημαντικές αδυναμίες που σχετίζονται με το υψηλό κόστος και το περιορισμένο πεδίο εφαρμογής της. Μέχρι σήμερα έχουν αναπτυχθεί μόνο λίγα προφίλ προστασίας για ψηφιακά προϊόντα, όπως η ψηφιακή υπογραφή, ο ψηφιακός ταχογράφος και οι έξυπνες κάρτες. Επιπλέον, η SOG-IS αφορά μόνο μέρος των κρατών μελών της ΕΕ. Αυτό περιορίζει την αποτελεσματικότητα της συμφωνίας αμοιβαίας αναγνώρισης της SOG-IS από την άποψη της εσωτερικής αγοράς.

(52) Λαμβανομένων υπόψη των ανωτέρω, είναι απαραίτητη η θέσπιση ενός ευρωπαϊκού πλαισίου πιστοποίησης της ασφάλειας στον κυβερνοχώρο που αφενός θα προβλέπει τις κύριες οριζόντιες απαιτήσεις για τα ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο που πρόκειται να αναπτυχθούν, και αφετέρου θα καθιστά δυνατή την αναγνώριση των πιστοποιητικών για προϊόντα και υπηρεσίες ΤΠΕ και τη χρήση αυτών σε όλα τα κράτη μέλη Το ευρωπαϊκό πλαίσιο θα πρέπει να έχει διττό σκοπό: αφενός, θα πρέπει να συμβάλλει στην ενίσχυση της εμπιστοσύνης σε προϊόντα και υπηρεσίες ΤΠΕ που έχουν λάβει πιστοποίηση σύμφωνα με αυτά τα συστήματα. Αφετέρου, θα πρέπει να αποφεύγει τις συγκρουόμενες ή αλληλεπικαλυπτόμενες εθνικές πιστοποιήσεις της ασφάλειας στον κυβερνοχώρο και, ως εκ τούτου, να περιορίζει το κόστος για τις επιχειρήσεις που δραστηριοποιούνται στην ψηφιακή ενιαία αγορά. Τα συστήματα δεν θα πρέπει να κάνουν διακρίσεις και θα πρέπει να βασίζονται σε διεθνή και/ή ενωσιακά πρότυπα, εκτός αν αυτά τα

πρότυπα είναι αναποτελεσματικά ή ακατάλληλα να καλύψουν τους σχετικούς θεμιτούς στόχους της ΕΕ.

(53) Η Επιτροπή θα πρέπει να εξουσιοδοτηθεί να εγκρίνει ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο όσον αφορά συγκεκριμένες ομάδες προϊόντων και υπηρεσιών ΤΠΕ. Αυτά τα συστήματα θα πρέπει να εφαρμόζονται και να επιβλέπονται από εθνικές εποπτικές αρχές πιστοποίησης και τα πιστοποιητικά που εκδίδονται στο πλαίσιο αυτών των συστημάτων θα πρέπει να είναι έγκυρα και να αναγνωρίζονται στο σύνολο της Ένωσης. Τα συστήματα πιστοποίησης που εφαρμόζονται από τη βιομηχανία ή άλλους ιδιωτικούς οργανισμούς δεν θα πρέπει να εμπίπτουν στο πεδίο εφαρμογής του κανονισμού. Ωστόσο, οι οργανισμοί που εφαρμόζουν τέτοια συστήματα μπορεί να προτείνουν στην Επιτροπή να εξετάσει αυτά τα συστήματα προκειμένου να εγκριθούν ως ευρωπαϊκά συστήματα.

(54) Οι διατάξεις του παρόντος κανονισμού δεν θα πρέπει να θίγουν την ενωσιακή νομοθεσία που προβλέπει συγκεκριμένους κανόνες για την πιστοποίηση προϊόντων και υπηρεσιών ΤΠΕ. Πιο συγκεκριμένα, ο γενικός κανονισμός για την προστασία δεδομένων (ΓΚΠΔ) περιλαμβάνει διατάξεις για τη θέσπιση μηχανισμών πιστοποίησης και σφραγίδων και σημάτων προστασίας των δεδομένων, προκειμένου να αποδεικνύεται η συμμόρφωση με τον εν λόγω κανονισμό των πράξεων επεξεργασίας από τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία. Αυτοί οι μηχανισμοί πιστοποίησης και οι σφραγίδες και τα σήματα προστασίας των δεδομένων θα πρέπει να επιτρέπουν στα υποκείμενα των δεδομένων να αξιολογούν ταχέως το επίπεδο προστασίας των δεδομένων των σχετικών προϊόντων και υπηρεσιών. Ο παρών κανονισμός ισχύει με την επιφύλαξη της πιστοποίησης των πράξεων επεξεργασίας των δεδομένων, ακόμη και όταν τέτοιες πράξεις βρίσκονται ενσωματωμένες σε προϊόντα και υπηρεσίες, στο πλαίσιο του ΓΚΠΔ.

(55) Σκοπός των ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο θα πρέπει να είναι να διασφαλίζουν ότι τα προϊόντα και οι υπηρεσίες ΤΠΕ που πιστοποιούνται στο πλαίσιο ενός τέτοιου συστήματος συμμορφώνονται με συγκεκριμένες απαιτήσεις. Τέτοιες απαιτήσεις αφορούν την ικανότητα ενός συστήματος να ανθίσταται, σε ένα δεδομένο επίπεδο διασφάλισης, σε ενέργειες οι οποίες θέτουν σε κίνδυνο τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα και την εμπιστευτικότητα αποθηκευμένων ή διαβιβαζόμενων ή επεξεργασμένων δεδομένων ή των σχετικών λειτουργιών ή των σχετικών υπηρεσιών που παρέχονται ή είναι προσβάσιμες μέσω των εν λόγω προϊόντων, διαδικασιών, υπηρεσιών και συστημάτων κατά την έννοια του παρόντος κανονισμού. Στον παρόντα κανονισμό δεν είναι δυνατόν να καθοριστούν λεπτομερώς οι απαιτήσεις ασφάλειας στον κυβερνοχώρο που σχετίζονται με το σύνολο των προϊόντων και των υπηρεσιών ΤΠΕ. Τα προϊόντα και οι υπηρεσίες ΤΠΕ και οι σχετικές ανάγκες ασφάλειας στον κυβερνοχώρο ποικίλουν σε τέτοιο βαθμό ώστε είναι πολύ δύσκολο να προβλεφθούν οριζόντιες γενικές απαιτήσεις ασφάλειας στον κυβερνοχώρο. Επομένως, είναι απαραίτητο να υιοθετηθεί μια ευρεία και γενική έννοια της ασφάλειας στον κυβερνοχώρο για τους σκοπούς της πιστοποίησης, η οποία θα συμπληρώνεται από ένα σύνολο συγκεκριμένων στόχων ασφάλειας στον κυβερνοχώρο που πρέπει να συνεκτιμώνται κατά τον σχεδιασμό των ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο. Οι λεπτομέρειες με τις οποίες θα επιτυγχάνονται αυτοί οι στόχοι για συγκεκριμένα προϊόντα και συγκεκριμένες υπηρεσίες ΤΠΕ θα πρέπει να διευκρινίζονται περαιτέρω αναλυτικώς στο επίπεδο του επιμέρους συστήματος πιστοποίησης που εγκρίνεται από την Επιτροπή, για παράδειγμα με αναφορά σε πρότυπα ή τεχνικές προδιαγραφές.

(56) Η Επιτροπή θα πρέπει να έχει τη δυνατότητα να ζητά από τον ENISA να επεξεργάζεται υποψήφια συστήματα για συγκεκριμένα προϊόντα ή συγκεκριμένες υπηρεσίες ΤΠΕ. Στη συνέχεια, με γνώμονα το υποψήφιο σύστημα που προτείνει ο ENISA, η Επιτροπή θα πρέπει να εξουσιοδοτείται να εγκρίνει το ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο μέσω εκτελεστικών πράξεων. Λαμβάνοντας υπόψη τον γενικό σκοπό και τους στόχους ασφάλειας που προβλέπονται στον παρόντα κανονισμό, τα ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο που εγκρίνονται από την Επιτροπή θα πρέπει να ορίζουν ένα ελάχιστο σύνολο στοιχείων όσον αφορά το αντικείμενο, το πεδίο εφαρμογής και τη λειτουργία του επιμέρους συστήματος. Αυτά θα πρέπει να περιλαμβάνουν μεταξύ άλλων το πεδίο εφαρμογής και το αντικείμενο της πιστοποίησης της ασφάλειας στον κυβερνοχώρο, συμπεριλαμβανομένων των καλυπτόμενων κατηγοριών των προϊόντων και των υπηρεσιών ΤΠΕ, τον λεπτομερή καθορισμό των απαιτήσεων ασφάλειας στον κυβερνοχώρο, για παράδειγμα με αναφορά σε πρότυπα ή τεχνικές προδιαγραφές, τα συγκεκριμένα κριτήρια αξιολόγησης και τις μεθόδους αξιολόγησης, καθώς και το επιθυμητό επίπεδο διασφάλισης: βασικό, σημαντικό και/ή υψηλό.

(57) Η προσφυγή στην ευρωπαϊκή πιστοποίηση της ασφάλειας στον κυβερνοχώρο θα πρέπει να παραμένει εθελοντική, εκτός αν ορίζεται άλλως στην ενωσιακή ή την εθνική νομοθεσία. Ωστόσο, προκειμένου να επιτυγχάνονται οι στόχοι του παρόντος κανονισμού και να αποφεύγεται ο κατακερματισμός της εσωτερικής αγοράς, τα εθνικά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο ή οι διαδικασίες για τα προϊόντα και τις υπηρεσίες ΤΠΕ που καλύπτονται από ένα ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο θα πρέπει να παύουν να ισχύουν από την ημερομηνία που ορίζεται με την εκτελεστική πράξη από την Επιτροπή. Επιπλέον, τα κράτη μέλη δεν θα πρέπει να θεσπίζουν νέα εθνικά συστήματα πιστοποίησης, τα οποία προβλέπουν συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο για προϊόντα και υπηρεσίες ΤΠΕ που καλύπτονται ήδη από υφιστάμενο ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο.

(58) Αφού εγκριθεί ένα ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο, οι κατασκευαστές προϊόντων ΤΠΕ ή οι πάροχοι υπηρεσιών ΤΠΕ θα πρέπει να είναι σε θέση να υποβάλλουν αίτηση πιστοποίησης των προϊόντων ή των υπηρεσιών τους σε έναν οργανισμό αξιολόγησης της συμμόρφωσης της επιλογής τους. Οι οργανισμοί αξιολόγησης της συμμόρφωσης θα πρέπει να είναι διαπιστευμένοι από οργανισμό διαπίστευσης, ώστε να πληρούν ορισμένες καθορισμένες απαιτήσεις που προβλέπονται στον παρόντα κανονισμό. Η διαπίστευση θα πρέπει να εκδίδεται για μέγιστη περίοδο πέντε ετών και μπορεί να ανανεωθεί με τους ίδιους όρους, υπό την προϋπόθεση ότι ο οργανισμός αξιολόγησης της συμμόρφωσης πληροί τις σχετικές απαιτήσεις. Οι οργανισμοί διαπίστευσης θα πρέπει να ανακαλούν τη διαπίστευση ενός οργανισμού αξιολόγησης της συμμόρφωσης σε περίπτωση που οι όροι διαπίστευσης δεν πληρούνται ή έχουν πάψει να πληρούνται, ή σε περίπτωση που τα μέτρα που λαμβάνει ένας οργανισμός αξιολόγησης της συμμόρφωσης παραβαίνουν τον παρόντα κανονισμό.

(59) Είναι αναγκαίο να απαιτείται από όλα τα κράτη μέλη να ορίζουν μία εποπτική αρχή πιστοποίησης της ασφάλειας στον κυβερνοχώρο, η οποία θα εποπτεύει τη συμμόρφωση αφενός των οργανισμών αξιολόγησης της συμμόρφωσης, και αφετέρου των πιστοποιητικών που εκδίδουν οι οργανισμοί αξιολόγησης της συμμόρφωσης που είναι εγκατεστημένοι στο έδαφός τους, με τις απαιτήσεις του παρόντος κανονισμού και των σχετικών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο. Οι

εθνικές εποπτικές αρχές πιστοποίησης θα πρέπει να χειρίζονται τις καταγγελίες που υποβάλλονται από φυσικά ή νομικά πρόσωπα σε σχέση με πιστοποιητικά που έχουν εκδοθεί από οργανισμούς αξιολόγησης της συμμόρφωσης που είναι εγκατεστημένοι στην επικράτειά τους, να εξετάζουν, στον βαθμό που κρίνεται απαραίτητο, το αντικείμενο της καταγγελίας και να ενημερώνουν τον καταγγέλλοντα όσον αφορά την πρόοδο και το αποτέλεσμα της έρευνας εντός εύλογου χρονικού διαστήματος. Επιπλέον, θα πρέπει να συνεργάζονται με άλλες εθνικές εποπτικές αρχές πιστοποίησης ή άλλη δημόσια αρχή, μεταξύ άλλων ανταλλάσσοντας πληροφορίες σχετικά με την πιθανή μη συμμόρφωση προϊόντων και υπηρεσιών ΤΠΕ με τις απαιτήσεις του παρόντος κανονισμού ή συγκεκριμένων συστημάτων ασφάλειας στον κυβερνοχώρο.

(60) Για να διασφαλιστεί η συνεκτική εφαρμογή του ευρωπαϊκού πλαισίου πιστοποίησης της ασφάλειας στον κυβερνοχώρο, θα πρέπει να δημιουργηθεί ευρωπαϊκή ομάδα πιστοποίησης της ασφάλειας στον κυβερνοχώρο (εφεξής η «ομάδα»), η οποία θα απαρτίζεται από τις εθνικές εποπτικές αρχές πιστοποίησης. Κύρια καθήκοντα της ομάδας θα είναι να συμβουλεύει και να επικουρεί την Επιτροπή στην προσπάθειά της να διασφαλίζει τη συνεπή υλοποίηση και εφαρμογή του ευρωπαϊκού πλαισίου πιστοποίησης της ασφάλειας στον κυβερνοχώρο· να συνδράμει και να συνεργάζεται στενά με τον Οργανισμό κατά την επεξεργασία των υποψήφιων συστημάτων πιστοποίησης ασφάλειας στον κυβερνοχώρο· να συστήνει στην Επιτροπή να ζητήσει από τον Οργανισμό την επεξεργασία ενός υποψήφιου ευρωπαϊκού συστήματος πιστοποίησης της ασφάλειας στον κυβερνοχώρο· και να εκδίδει γνώμες απευθυνόμενες στην Επιτροπή όσον αφορά τη διατήρηση και την επανεξέταση υφιστάμενων ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο.

(61) Για να προάγει την ευαισθητοποίηση και να διευκολύνει την αποδοχή μελλοντικών ευρωπαϊκών συστημάτων ασφάλειας στον κυβερνοχώρο, η Ευρωπαϊκή Επιτροπή μπορεί να εκδίδει γενικές ή ειδικές ανά τομέα κατευθυντήριες γραμμές για την ασφάλεια στον κυβερνοχώρο, π.χ. σχετικά με τις ορθές πρακτικές ή την υπεύθυνη συμπεριφορά για την ασφάλεια στον κυβερνοχώρο, υπογραμμίζοντας το θετικό αποτέλεσμα από τη χρήση πιστοποιημένων προϊόντων και υπηρεσιών ΤΠΕ.

(62) Η υποστήριξη του Οργανισμού στην πιστοποίηση της ασφάλειας στον κυβερνοχώρο θα πρέπει επίσης να περιλαμβάνει τη συνεργασία με την Επιτροπή Ασφαλείας του Συμβουλίου και τον αρμόδιο εθνικό φορέα, όσον αφορά την κρυπτογραφική έγκριση προϊόντων που πρόκειται να χρησιμοποιηθούν σε διαβαθμισμένα δίκτυα.

(63) Προκειμένου να προσδιοριστούν περαιτέρω τα κριτήρια για τη διαπίστευση των οργανισμών αξιολόγησης της συμμόρφωσης, θα πρέπει να ανατεθεί στην Επιτροπή η εξουσία έκδοσης πράξεων σύμφωνα με το άρθρο 290 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης. Η Επιτροπή θα πρέπει να διεξάγει, κατά τις προπαρασκευαστικές της εργασίες, τις κατάλληλες διαβουλεύσεις, μεταξύ άλλων σε επίπεδο εμπειρογνωμόνων. Οι εν λόγω διαβουλεύσεις θα πρέπει να πραγματοποιούνται σύμφωνα με τις αρχές που ορίζονται στη διοργανική συμφωνία για τη βελτίωση του νομοθετικού έργου της 13ης Απριλίου 2016. Πιο συγκεκριμένα, προκειμένου να εξασφαλιστεί η ίση συμμετοχή στην προετοιμασία των κατ' εξουσιοδότηση πράξεων, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο θα πρέπει να 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.

(64) Για τη διασφάλιση ενιαίων προϋποθέσεων εφαρμογής του παρόντος κανονισμού θα πρέπει να ανατεθούν εκτελεστικές αρμοδιότητες στην Επιτροπή όταν προβλέπεται από τον παρόντα κανονισμό. Οι εν λόγω αρμοδιότητες θα πρέπει να ασκούνται σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 182/2011.

(65) Η διαδικασία εξέτασης θα πρέπει να χρησιμοποιείται για την έγκριση των εκτελεστικών πράξεων σχετικά με τα ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο για προϊόντα και υπηρεσίες ΤΠΕ, σχετικά με τις λεπτομέρειες διενέργειας ερευνών από τον Οργανισμό, καθώς και σχετικά με τις περιστάσεις, τους μορφότυπους και τις διαδικασίες που ισχύουν για τις κοινοποιήσεις των διαπιστευμένων οργανισμών αξιολόγησης της συμμόρφωσης από τις εθνικές εποπτικές αρχές πιστοποίησης στην Επιτροπή.

(66) Το έργο του Οργανισμού θα πρέπει να αξιολογείται ανεξάρτητα. Στην αξιολόγηση θα πρέπει να λαμβάνονται υπόψη η αποτελεσματικότητα του Οργανισμού στην επίτευξη των στόχων του, οι εργασιακές πρακτικές του και η συνάφεια των καθηκόντων του. Η αξιολόγηση θα πρέπει επίσης να εκτιμά τον αντίκτυπο, την αποτελεσματικότητα και την αποδοτικότητα του ευρωπαϊκού πλαισίου πιστοποίησης της ασφάλειας στον κυβερνοχώρο.

(67) Ο κανονισμός (ΕΕ) αριθ. 526/2013 θα πρέπει να καταργηθεί.

(68) Δεδομένου ότι οι στόχοι του παρόντος κανονισμού δεν μπορούν να επιτευχθούν επαρκώς από τα κράτη μέλη, μπορούν όμως να επιτευχθούν καλύτερα στο επίπεδο της Ένωσης, η Ένωση μπορεί να θεσπίσει μέτρα σύμφωνα με την αρχή της επικουρικότητας, όπως αυτή διατυπώνεται στο άρθρο 5 της Συνθήκης για την Ευρωπαϊκή Ένωση. Σύμφωνα με την αρχή της αναλογικότητας, που ορίζεται στο ίδιο άρθρο, ο παρών κανονισμός δεν υπερβαίνει τα απαιτούμενα για την επίτευξη του στόχου αυτού,

ΕΞΕΔΩΣΑΝ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

ΤΙΤΛΟΣ Ι
ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 1
Αντικείμενο και πεδίο εφαρμογής

Προκειμένου να εξασφαλίζεται η ορθή λειτουργία της εσωτερικής αγοράς, σε συνδυασμό με ένα υψηλό επίπεδο ασφάλειας, ανθεκτικότητας και εμπιστοσύνης στον κυβερνοχώρο εντός της Ένωσης, ο παρών κανονισμός:

α) καθορίζει τους στόχους, τα καθήκοντα και τις οργανωτικές πτυχές του ENISA, του «Οργανισμού της ΕΕ για την ασφάλεια στον κυβερνοχώρο», στο εξής ο «Οργανισμός»· και

β) καθορίζει πλαίσιο για τη θέσπιση ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο με σκοπό τη διασφάλιση επαρκούς επιπέδου ασφάλειας στον κυβερνοχώρο προϊόντων και υπηρεσιών ΤΠΕ στην Ένωση. Ένα τέτοιο πλαίσιο εφαρμόζεται με την επιφύλαξη συγκεκριμένων διατάξεων σε σχέση με την εθελοντική ή την υποχρεωτική πιστοποίηση σε άλλες πράξεις της Ένωσης.

Άρθρο 2
Ορισμοί

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

(1) «ασφάλεια στον κυβερνοχώρο»: όλες οι δραστηριότητες που απαιτούνται για την προστασία των συστημάτων δικτύου και πληροφοριών, των χρηστών τους και των επηρεαζόμενων ατόμων από απειλές στον κυβερνοχώρο·

(2) «σύστημα δικτύου και πληροφοριών»: σύστημα κατά την έννοια του άρθρου 4 σημείο 1) της οδηγίας (ΕΕ) 2016/1148·

(3) «εθνική στρατηγική για την ασφάλεια συστημάτων δικτύου και πληροφοριών»: πλαίσιο κατά την έννοια του άρθρου 4 σημείο 3) της οδηγίας (ΕΕ) 2016/1148·

(4) «φορέας εκμετάλλευσης βασικών υπηρεσιών»: δημόσια ή ιδιωτική οντότητα όπως ορίζεται στο άρθρο 4 σημείο 4) της οδηγίας (ΕΕ) 2016/1148·

(5) «πάροχος ψηφιακών υπηρεσιών»: κάθε νομικό πρόσωπο που παρέχει ψηφιακή υπηρεσία, όπως ορίζεται στο άρθρο 4 σημείο 6 της οδηγίας (ΕΕ) 2016/1148·

(6) «συμβάν»: κάθε γεγονός όπως ορίζεται στο άρθρο 4 σημείο 7) της οδηγίας (ΕΕ) 2016/1148·

(7) «χειρισμός συμβάντων»: κάθε διαδικασία όπως ορίζεται στο άρθρο 4 σημείο 8) της οδηγίας (ΕΕ) 2016/1148·

(8) «απειλή στον κυβερνοχώρο»: κάθε πιθανή περίσταση ή πιθανό συμβάν που μπορεί να επιδράσει δυσμενώς στα συστήματα δικτύου και πληροφοριών, στους χρήστες τους και στα επηρεαζόμενα άτομα.

(9) «ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο»: το πλήρες σύνολο κανόνων, τεχνικών απαιτήσεων, προτύπων και διαδικασιών το οποίο ορίζεται σε επίπεδο Ένωσης και εφαρμόζεται για την πιστοποίηση των προϊόντων και των υπηρεσιών τεχνολογίας των πληροφοριών και των επικοινωνιών (ΤΠΕ) που εμπίπτουν στο πεδίο εφαρμογής του συγκεκριμένου συστήματος·

(10) «ευρωπαϊκό πιστοποιητικό ασφάλειας στον κυβερνοχώρο»: έγγραφο που εκδίδει ένας οργανισμός αξιολόγησης της συμμόρφωσης, το οποίο βεβαιώνει ότι ένα συγκεκριμένο προϊόν ή μια συγκεκριμένη υπηρεσία ΤΠΕ πληροί τις ειδικές απαιτήσεις που προβλέπει ένα ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο·

(11) «προϊόν και υπηρεσία ΤΠΕ»: κάθε στοιχείο ή ομάδα στοιχείων των συστημάτων δικτύου και πληροφοριών·

(12) «διαπίστευση»: η διαπίστευση όπως ορίζεται στο άρθρο 2 σημείο 10) του κανονισμού (ΕΚ) αριθ. 765/2008·

(13) «εθνικός οργανισμός διαπίστευσης»: ο εθνικός οργανισμός διαπίστευσης όπως ορίζεται στο άρθρο 2 σημείο 11) του κανονισμού (ΕΚ) αριθ. 765/2008·

(14) «αξιολόγηση της συμμόρφωσης»: αξιολόγηση της συμμόρφωσης όπως ορίζεται στο άρθρο 2 σημείο 12) του κανονισμού (ΕΚ) αριθ. 765/2008·

(15) «οργανισμός αξιολόγησης της συμμόρφωσης»: οργανισμός αξιολόγησης της συμμόρφωσης όπως ορίζεται στο άρθρο 2 σημείο 13) του κανονισμού (ΕΚ) αριθ. 765/2008·

(16) «πρότυπο»: πρότυπο όπως ορίζεται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΕ) αριθ. 1025/2012.

ΤΙΤΛΟΣ ΙΙ

ENISA – ο «Οργανισμός της ΕΕ για την ασφάλεια στον κυβερνοχώρο»

ΚΕΦΑΛΑΙΟ Ι
ΕΝΤΟΛΗ, ΣΤΟΧΟΙ ΚΑΙ ΚΑΘΗΚΟΝΤΑ

Άρθρο 3
Εντολή

1. Ο Οργανισμός αναλαμβάνει τα καθήκοντα που του ανατίθενται με τον παρόντα κανονισμό με σκοπό να συμβάλει σε ένα υψηλό επίπεδο ασφάλειας στον κυβερνοχώρο εντός της Ένωσης.

2. Ο Οργανισμός ασκεί καθήκοντα που του ανατίθενται με πράξεις της Ένωσης σχετικά με τον καθορισμό μέτρων για την προσέγγιση νόμων, κανονισμών και διοικητικών διατάξεων των κρατών μελών που σχετίζονται με την ασφάλεια στον κυβερνοχώρο.

3. Οι στόχοι και τα καθήκοντα του Οργανισμού δεν θίγουν τις αρμοδιότητες των κρατών μελών σχετικά με την ασφάλεια στον κυβερνοχώρο ούτε, σε κάθε περίπτωση, τις δραστηριότητες που αφορούν τη δημόσια ασφάλεια, την άμυνα, την εθνική ασφάλεια και τις δραστηριότητες του κράτους σε τομείς του ποινικού δικαίου.

Άρθρο 4
Στόχοι

1. Ο Οργανισμός αποτελεί κέντρο εμπειρογνωσίας σε θέματα ασφάλειας στον κυβερνοχώρο χάρη στην ανεξαρτησία του, την επιστημονική και τεχνική ποιότητα των συμβουλών και της επικουρίας, καθώς και των πληροφοριών. που παρέχει, τη διαφάνεια των επιχειρησιακών διαδικασιών και μεθόδων λειτουργίας του και την επιμέλεια με την οποία εκτελεί τα καθήκοντά του.

2. Ο Οργανισμός επικουρεί τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης, καθώς και τα κράτη μέλη, στην ανάπτυξη και την εφαρμογή πολιτικών που σχετίζονται με την ασφάλεια στον κυβερνοχώρο.

3. Ο Οργανισμός στηρίζει την ανάπτυξη ικανοτήτων και την ετοιμότητα στην Ένωση, επικουρώντας την Ένωση, τα κράτη μέλη και τους ιδιωτικούς και δημόσιους άμεσα ενδιαφερόμενους, με σκοπό την ενίσχυση της προστασίας των συστημάτων δικτύου και πληροφοριών τους, την ανάπτυξη δεξιοτήτων και ικανοτήτων στο πεδίο της ασφάλειας στον κυβερνοχώρο και την επίτευξη ανθεκτικότητας στον κυβερνοχώρο.

4. Ο Οργανισμός προάγει τη συνεργασία και τον συντονισμό σε ενωσιακό επίπεδο ανάμεσα στα κράτη μέλη, τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης, καθώς και στους σχετικούς άμεσα ενδιαφερόμενους, συμπεριλαμβανομένου του ιδιωτικού τομέα, σε θέματα που σχετίζονται με την ασφάλεια στον κυβερνοχώρο.

5. Ο Οργανισμός αυξάνει τις δυνατότητες ασφάλειας στον κυβερνοχώρο σε επίπεδο Ένωσης προκειμένου να συμπληρώνει τη δράση των κρατών μελών όσον αφορά την

πρόληψη και την αντιμετώπιση απειλών στον κυβερνοχώρο, κυρίως σε περίπτωση διασυνοριακών συμβάντων.

6. Ο Οργανισμός προάγει τη χρήση της πιστοποίησης, συμβάλλοντας, μεταξύ άλλων, στη θέσπιση και τη διατήρηση ενός πλαισίου πιστοποίησης της ασφάλειας στον κυβερνοχώρο σε επίπεδο Ένωσης σύμφωνα με τον τίτλο ΙΙΙ του παρόντος κανονισμού, προκειμένου να αυξηθεί η διαφάνεια της διασφάλισης της ασφάλειας στον κυβερνοχώρο των προϊόντων και υπηρεσιών ΤΠΕ και, επομένως, να ενισχυθεί η εμπιστοσύνη στην ψηφιακή εσωτερική αγορά.

7. Ο Οργανισμός προάγει ένα υψηλό επίπεδο ευαισθητοποίησης των πολιτών και των επιχειρήσεων σε θέματα που σχετίζονται με την ασφάλεια στον κυβερνοχώρο.

Άρθρο 5

Καθήκοντα σχετικά με τη χάραξη και την εφαρμογή της πολιτικής και της νομοθεσίας της Ένωσης

Ο Οργανισμός συμβάλλει στη χάραξη και την εφαρμογή της πολιτικής και της νομοθεσίας της Ένωσης:

1. επικουρώντας και παρέχοντας συμβουλές, κυρίως με την παροχή ανεξάρτητης γνωμοδότησης και προπαρασκευαστικών εργασιών σχετικά με τη χάραξη και την επανεξέταση της πολιτικής και της νομοθεσίας της Ένωσης στον τομέα της ασφάλειας στον κυβερνοχώρο, καθώς και των πρωτοβουλιών πολιτικής και νομοθεσίας ανά τομέα εφόσον εμπλέκονται ζητήματα που αφορούν την ασφάλεια στον κυβερνοχώρο·

2. επικουρώντας τα κράτη μέλη για τη συνεπή εφαρμογή της πολιτικής και της νομοθεσίας της Ένωσης σχετικά με την ασφάλεια στον κυβερνοχώρο, ιδίως σε σχέση με την οδηγία (ΕΕ) 2016/1148, μεταξύ άλλων με γνωμοδοτήσεις, κατευθυντήριες γραμμές, συμβουλές και βέλτιστες πρακτικές σχετικά με ζητήματα όπως διαχείριση κινδύνων, κοινοποίηση συμβάντων και ανταλλαγή πληροφοριών, καθώς και διευκολύνοντας την ανταλλαγή βέλτιστων πρακτικών μεταξύ αρμόδιων αρχών για το θέμα αυτό·

3. συμβάλλοντας στο έργο της ομάδας συνεργασίας δυνάμει του άρθρου 11 της οδηγίας (ΕΕ) 2016/1148, παρέχοντας την εμπειρογνωσία και τη συνδρομή του·

4. στηρίζοντας:

   (1) τη χάραξη και την εφαρμογή της ενωσιακής πολιτικής στον τομέα της ηλεκτρονικής ταυτότητας και των υπηρεσιών εμπιστοσύνης, κυρίως με την παροχή συμβουλών και τεχνικών κατευθυντήριων γραμμών, καθώς και με τη διευκόλυνση της ανταλλαγής βέλτιστων πρακτικών μεταξύ αρμόδιων αρχών·

   (2) την προαγωγή ενισχυμένου επιπέδου ασφάλειας των ηλεκτρονικών επικοινωνιών, μεταξύ άλλων με την παροχή εμπειρογνωσίας και συμβουλών, καθώς και με τη διευκόλυνση της ανταλλαγής βέλτιστων πρακτικών μεταξύ αρμόδιων αρχών·

5. στηρίζοντας την τακτική επανεξέταση των δραστηριοτήτων πολιτικής της Ένωσης με την παροχή ετήσιας έκθεσης σχετικά με την κατάσταση εφαρμογής του αντίστοιχου νομικού πλαισίου όσον αφορά:

α) τις κοινοποιήσεις συμβάντων των κρατών μελών που υποβάλλουν τα ενιαία κέντρα επαφής στην ομάδα συνεργασίας δυνάμει του άρθρου 10 παράγραφος 3 της οδηγίας (ΕΕ) 2016/1147·

β) τις κοινοποιήσεις παραβίασης της ασφάλειας και απώλειας της ακεραιότητας σε σχέση με τους παρόχους υπηρεσιών εμπιστοσύνης που υποβάλλουν τα εποπτικά όργανα στον Οργανισμό, δυνάμει του άρθρου 19 παράγραφος 3 του κανονισμού (ΕΕ) αριθ. 910/2014·

γ) τις κοινοποιήσεις παραβίασης της ασφάλειας που διαβιβάζουν οι επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών ή διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών, τις οποίες υποβάλλουν οι αρμόδιες αρχές στον Οργανισμό, δυνάμει του άρθρου 40 της [οδηγίας για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών].

Άρθρο 6

Καθήκοντα σχετικά με την ανάπτυξη ικανοτήτων

1. Ο Οργανισμός επικουρεί:

α) τα κράτη μέλη στις προσπάθειές τους να βελτιώσουν την ικανότητα πρόληψης, εντοπισμού και ανάλυσης, καθώς και την ικανότητα αντιμετώπισης προβλημάτων και συμβάντων σχετικών με την ασφάλεια στον κυβερνοχώρο, διαθέτοντάς τους τις απαιτούμενες γνώσεις και την απαιτούμενη εμπειρογνωσία·

β) τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης στις προσπάθειές τους να βελτιώσουν την ικανότητα πρόληψης, εντοπισμού και ανάλυσης, καθώς και την ικανότητα αντιμετώπισης προβλημάτων και συμβάντων σχετικών με την ασφάλεια στον κυβερνοχώρο, με την κατάλληλη υποστήριξη της ομάδας αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT) για τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης (CERT-EU)·

γ) τα κράτη μέλη, κατόπιν αιτήματός τους, στην ανάπτυξη εθνικών ομάδων απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT), δυνάμει του άρθρου 9 παράγραφος 5 της οδηγίας (ΕΕ) 2016/1148·

δ) τα κράτη μέλη, κατόπιν αιτήματός τους, στην ανάπτυξη εθνικών στρατηγικών για την ασφάλεια συστημάτων δικτύου και πληροφοριών, δυνάμει του άρθρου 7 παράγραφος 2 της οδηγίας (ΕΕ) 2016/1148, ο Οργανισμός προάγει επίσης τη διάδοση και παρακολουθεί την πρόοδο της εφαρμογής των εν λόγω στρατηγικών στην Ένωση, με σκοπό την προαγωγή των βέλτιστων πρακτικών·

ε) τα θεσμικά όργανα της Ένωσης στην ανάπτυξη και την επανεξέταση των ενωσιακών στρατηγικών για την ασφάλεια στον κυβερνοχώρο, προάγοντας τη διάδοσή τους και παρακολουθώντας την πρόοδο εφαρμογής τους·

στ) τις εθνικές και ενωσιακές CSIRT με στόχο την αύξηση του επιπέδου ικανότητάς τους, μεταξύ άλλων με την προώθηση του διαλόγου και της ανταλλαγής πληροφοριών, προκειμένου να εξασφαλίζεται ότι, όσον αφορά τη διαθέσιμη τεχνολογία αιχμής, κάθε CSIRT διαθέτει ένα κοινό σύνολο ελάχιστων ικανοτήτων και λειτουργεί με βάση τις βέλτιστες πρακτικές·

ζ) τα κράτη μέλη μέσω της οργάνωσης ετήσιων μεγάλης κλίμακας ασκήσεων ασφάλειας στον κυβερνοχώρο σε επίπεδο Ένωσης, όπως αναφέρονται στο άρθρο 7 παράγραφος 6, και με τη διατύπωση συστάσεων πολιτικής βάσει της διαδικασίας αξιολόγησης των ασκήσεων και των διδαγμάτων που αποκομίζονται από αυτές·

η) τους αρμόδιους δημόσιους οργανισμούς με την παροχή κατάρτισης σχετικά με την ασφάλεια στον κυβερνοχώρο, και αν κρίνεται σκόπιμο σε συνεργασία με τους άμεσα ενδιαφερόμενους·

θ) την ομάδα συνεργασίας, μέσω της ανταλλαγής βέλτιστων πρακτικών, ιδίως όσον αφορά τον προσδιορισμό των φορέων εκμετάλλευσης βασικών υπηρεσιών από τα κράτη μέλη, συμπεριλαμβανομένων μεταξύ άλλων όσον αφορά διασυνοριακές εξαρτήσεις σε σχέση με κινδύνους και συμβάντα, δυνάμει του άρθρου 11 παράγραφος 3 στοιχείο ιβ) της οδηγίας (ΕΕ) 2016/1148.

2. Ο Οργανισμός διευκολύνει τη θέσπιση και τη διαρκή στήριξη των τομεακών κέντρων κοινοχρησίας και ανάλυσης πληροφοριών (ISAC), ιδίως στους τομείς που παρατίθενται στο παράρτημα ΙΙ της οδηγίας (ΕΕ) 2016/1148, με την παροχή βέλτιστων πρακτικών και καθοδήγησης για τα διαθέσιμα εργαλεία, τη διαδικασία, καθώς και τον τρόπο αντιμετώπισης των ρυθμιστικών ζητημάτων που σχετίζονται με την ανταλλαγή πληροφοριών.

Άρθρο 7

Καθήκοντα σχετικά με την επιχειρησιακή συνεργασία σε επίπεδο Ένωσης

1. Ο Οργανισμός υποστηρίζει την επιχειρησιακή συνεργασία μεταξύ αρμόδιων δημόσιων αρχών και μεταξύ άμεσα ενδιαφερομένων.

2. Ο Οργανισμός συνεργάζεται σε επιχειρησιακό επίπεδο και αναπτύσσει συνέργειες με τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης, συμπεριλαμβανομένων της CERT-EU, των υπηρεσιών που ασχολούνται με το ηλεκτρονικό έγκλημα και των εποπτικών αρχών που ασχολούνται με την προστασία της ιδιωτικότητας και των δεδομένων προσωπικού χαρακτήρα, με σκοπό την αντιμετώπιση κοινών προβλημάτων, μεταξύ άλλων:

   α) την ανταλλαγή τεχνογνωσίας και βέλτιστων πρακτικών·

   β) την παροχή συμβουλών και κατευθυντήριων γραμμών σχετικά με συναφή θέματα που σχετίζονται με την ασφάλεια στον κυβερνοχώρο·

   γ) τη θέσπιση, κατόπιν διαβούλευσης με την Επιτροπή, πρακτικών ρυθμίσεων για την εκτέλεση συγκεκριμένων καθηκόντων.

3. Ο Οργανισμός παρέχει γραμματειακή υποστήριξη στο δίκτυο CSIRT, δυνάμει του άρθρου 12 παράγραφος 2 της οδηγίας (ΕΕ) 2016/1148 και διευκολύνει ενεργά την ανταλλαγή πληροφοριών και τη συνεργασία μεταξύ των μελών του.

4. Ο Οργανισμός συμβάλλει στην επιχειρησιακή συνεργασία εντός του δικτύου CSIRT εξασφαλίζοντας στήριξη στα κράτη μέλη, με:

   α) την παροχή συμβουλών για τον τρόπο βελτίωσης των ικανοτήτων τους να προβλέπουν, να εντοπίζουν και να αντιμετωπίζουν συμβάντα·

β) την παροχή, κατόπιν αιτήματός τους, τεχνικής συνδρομής σε περίπτωση συμβάντων με σημαντικό ή ουσιαστικό αντίκτυπο·

γ) την ανάλυση τρωτών σημείων, σφαλμάτων και συμβάντων.

Κατά την εκτέλεση αυτών των καθηκόντων, ο Οργανισμός και η CERT-EU δεσμεύονται σε μια δομημένη συνεργασία προκειμένου να επωφελούνται από τις συνέργειες, ιδίως σε σχέση με τις επιχειρησιακές πτυχές.

5. Κατόπιν αιτήματος δύο ή περισσότερων οικείων κρατών μελών και με μοναδικό σκοπό την παροχή συμβουλών για την πρόληψη μελλοντικών συμβάντων, ο Οργανισμός παρέχει στήριξη ή διενεργεί εκ των προτέρων τεχνική έρευνα κατόπιν κοινοποιήσεων από επιχειρήσεις που επηρεάζονται από συμβάντα με σημαντικό ή ουσιαστικό αντίκτυπο, δυνάμει της οδηγίας (ΕΕ) 2016/1148. Ο Οργανισμός διενεργεί επίσης ανάλογη έρευνα κατόπιν δεόντως αιτιολογημένου αιτήματος από την Επιτροπή, σε συμφωνία με τα οικεία κράτη μέλη, σε περίπτωση τέτοιων συμβάντων που επηρεάζουν περισσότερα από δύο κράτη μέλη.

   Το πεδίο εφαρμογής της έρευνας και η διαδικασία που ακολουθείται κατά τη διενέργεια της έρευνας συμφωνούνται από τα οικεία κράτη μέλη και τον Οργανισμό και τελούν υπό την επιφύλαξη τυχόν ποινικών ερευνών που είναι σε εξέλιξη όσον αφορά το ίδιο συμβάν. Η έρευνα ολοκληρώνεται με μια τελική τεχνική έκθεση που συντάσσεται από τον Οργανισμό, ιδίως βάσει των πληροφοριών και των παρατηρήσεων που υποβάλλουν τα οικεία κράτη μέλη και η/οι επιχείρηση/επιχειρήσεις και συμφωνούνται με τα οικεία κράτη μέλη. Μια περίληψη της έκθεσης που εστιάζει στις συστάσεις για την πρόληψη μελλοντικών συμβάντων θα κοινοποιείται στο δίκτυο CSIRT.

6. Ο Οργανισμός οργανώνει ετήσιες ασκήσεις ασφάλειας στον κυβερνοχώρο σε επίπεδο Ένωσης και συνδράμει όλα τα κράτη μέλη και τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ στην οργάνωση ασκήσεων κατόπιν αιτήματός (αιτημάτων) τους. Οι ετήσιες ασκήσεις σε επίπεδο Ένωσης περιλαμβάνουν τεχνικά, επιχειρησιακά και στρατηγικά στοιχεία, καθώς και βοήθεια στην προετοιμασία μιας κοινής αντιμετώπισης για μεγάλης κλίμακας διασυνοριακά συμβάντα ασφάλειας στον κυβερνοχώρο σε επίπεδο Ένωσης. Επιπλέον, ο Οργανισμός συμβάλλει και συνδράμει στην οργάνωση, αν κρίνεται σκόπιμο, των τομεακών ασκήσεων ασφάλειας στον κυβερνοχώρο μαζί με αρμόδια ISAC και επιτρέπει στα ISAC να συμμετέχουν επίσης στις ασκήσεις ασφάλειας στον κυβερνοχώρο σε επίπεδο Ένωσης.

7. Ο Οργανισμός εκπονεί τακτική έκθεση για την τεχνική κατάσταση της ασφάλειας στον κυβερνοχώρο σε επίπεδο ΕΕ σχετικά με τα συμβάντα και τις απειλές, με βάση πληροφορίες ανοικτής πηγής, τις δικές του αναλύσεις και εκθέσεις που υποβάλλουν, μεταξύ άλλων: οι CSIRT των κρατών μελών (σε εθελοντική βάση) ή τα ενιαία κέντρα επαφής της οδηγίας για την ασφάλεια δικτύων και πληροφοριών (σύμφωνα με το άρθρο 14 παράγραφος 5 της οδηγίας για την ασφάλεια δικτύων και πληροφοριών)· το Ευρωπαϊκό Κέντρο για τα Εγκλήματα στον Κυβερνοχώρο (EC3) στο πλαίσιο της Ευρωπόλ, η CERT-EU.

8. Ο Οργανισμός συμβάλλει στην ανάπτυξη μιας κοινής αντιμετώπισης, σε επίπεδο Ένωσης και κρατών μελών, των μεγάλης κλίμακας συμβάντων και κρίσεων που αφορούν την ασφάλεια στον κυβερνοχώρο, κυρίως με:

α) τη συγκέντρωση εκθέσεων από εθνικές πηγές προκειμένου να συνεισφέρει στη δημιουργία κοινής επίγνωσης της κατάστασης·

β) τη διασφάλιση της αποτελεσματικής ροής πληροφοριών και της προμήθειας μηχανισμών κλιμάκωσης ανάμεσα στο δίκτυο CSIRT και στους υπευθύνους λήψης τεχνικών και πολιτικών αποφάσεων σε επίπεδο Ένωσης·

γ) την υποστήριξη του τεχνικού χειρισμού ενός συμβάντος ή μιας κρίσης, συμπεριλαμβανομένης της διευκόλυνσης της ανταλλαγής τεχνικών λύσεων μεταξύ κρατών μελών·

δ) την υποστήριξη της δημόσιας επικοινωνίας σχετικά με το συμβάν ή την κρίση·

ε) τη δοκιμασία των προγραμμάτων συνεργασίας για την αντιμετώπιση τέτοιων συμβάντων ή κρίσεων.

Άρθρο 8

Καθήκοντα σχετικά με την αγορά, την πιστοποίηση της ασφάλειας στον κυβερνοχώρο και την προτυποποίηση

Ο Οργανισμός:

α) υποστηρίζει και προάγει τη χάραξη και την εφαρμογή της πολιτικής της Ένωσης για την πιστοποίηση της ασφάλειας στον κυβερνοχώρο για προϊόντα και υπηρεσίες ΤΠΕ, όπως προβλέπεται στον τίτλο ΙΙΙ του παρόντος κανονισμού,:

(1) με την επεξεργασία υποψήφιων ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο για προϊόντα και υπηρεσίες ΤΠΕ, σύμφωνα με το άρθρο 44 του παρόντος κανονισμού·

(2) επικουρώντας την Επιτροπή, μέσω της παροχής γραμματειακής υποστήριξης στην ευρωπαϊκή ομάδα πιστοποίησης της ασφάλειας στον κυβερνοχώρο δυνάμει του άρθρου 53 του παρόντος κανονισμού·

(3) με τη σύνταξη και τη δημοσίευση κατευθυντήριων γραμμών και την ανάπτυξη ορθών πρακτικών σχετικά με τις απαιτήσεις ασφάλειας στον κυβερνοχώρο για προϊόντα και υπηρεσίες ΤΠΕ, σε συνεργασία με εθνικές εποπτικές αρχές πιστοποίησης και τη βιομηχανία·

β) με τη διευκόλυνση της θέσπισης και της αφομοίωσης ευρωπαϊκών και διεθνών προτύπων για τη διαχείριση κινδύνων και την ασφάλεια προϊόντων και υπηρεσιών ΤΠΕ, καθώς και με την εκπόνηση, σε συνεργασία με τα κράτη μέλη, συμβουλών και κατευθυντήριων γραμμών σχετικά με τα τεχνικά πεδία που αφορούν τις απαιτήσεις ασφάλειας των φορέων εκμετάλλευσης βασικών υπηρεσιών και των παρόχων ψηφιακών υπηρεσιών, αλλά και ήδη υφιστάμενα πρότυπα συμπεριλαμβανομένων των εθνικών προτύπων των κρατών μελών, δυνάμει του άρθρου 19 παράγραφος 2 της οδηγίας (ΕΕ) 2016/1148·

γ) με τη διενέργεια και τη διάδοση τακτικών αναλύσεων των κύριων τάσεων στην αγορά της ασφάλειας στον κυβερνοχώρο από την πλευρά τόσο της ζήτησης όσο και της προσφοράς, με σκοπό την ενίσχυση της αγοράς ασφάλειας στον κυβερνοχώρο εντός της Ένωσης.

Άρθρο 9

Καθήκοντα σχετικά με τις γνώσεις, τις πληροφορίες και την ευαισθητοποίηση

Ο Οργανισμός:

α) διενεργεί αναλύσεις των αναδυόμενων τεχνολογιών και παρέχει αξιολογήσεις για συγκεκριμένα θέματα σχετιζόμενα με τις αναμενόμενες κοινωνικές, νομικές, οικονομικές και ρυθμιστικές επιπτώσεις των τεχνολογικών καινοτομιών της ασφάλειας στον κυβερνοχώρο·

β) διενεργεί μακροπρόθεσμες στρατηγικές αναλύσεις των απειλών και των συμβάντων που αφορούν την ασφάλεια στον κυβερνοχώρο, προκειμένου να εντοπίζει τις αναδυόμενες τάσεις και να συμβάλλει στην πρόληψη προβλημάτων που σχετίζονται με την ασφάλεια στον κυβερνοχώρο·

γ) παρέχει, σε συνεργασία με εμπειρογνώμονες από τις αρχές των κρατών μελών, συμβουλές, καθοδήγηση και βέλτιστες πρακτικές για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, ιδίως για την ασφάλεια της υποδομής του διαδικτύου και εκείνων των υποδομών που υποστηρίζουν τους τομείς που αναφέρονται στο παράρτημα ΙΙ της οδηγίας (ΕΕ) 2016/1148·

δ) συγκεντρώνει, οργανώνει και γνωστοποιεί στο κοινό, μέσω ειδικής πύλης, πληροφορίες σχετικά με την ασφάλεια στον κυβερνοχώρο τις οποίες παρέχουν τα θεσμικά όργανα και λοιπά όργανα και οι οργανισμοί της Ένωσης·

ε) ευαισθητοποιεί το κοινό σχετικά με τους κινδύνους ασφάλειας στον κυβερνοχώρο και παρέχει καθοδήγηση σχετικά με τις ορθές πρακτικές για τους μεμονωμένους χρήστες στοχεύοντας σε πολίτες και οργανώσεις·

στ) συλλέγει και αναλύει δημόσια διαθέσιμες πληροφορίες σχετικά με σημαντικά συμβάντα και συντάσσει εκθέσεις με σκοπό την παροχή καθοδήγησης σε επιχειρήσεις και πολίτες στην Ένωση·

ζ) διοργανώνει, σε συνεργασία με τα κράτη μέλη και τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης, τακτικές εκστρατείες προβολής για την αύξηση της ασφάλειας στον κυβερνοχώρο και της ορατότητάς της στην Ένωση.

Άρθρο 10

Καθήκοντα σχετικά με την έρευνα και καινοτομία

Αναφορικά με την έρευνα και καινοτομία, ο Οργανισμός:

α) παρέχει υπηρεσίες συμβούλου στην Ένωση και τα κράτη μέλη σχετικά με ερευνητικές ανάγκες και προτεραιότητες στον τομέα της ασφάλειας στον κυβερνοχώρο, με σκοπό να καταστεί δυνατή η αποτελεσματική απόκριση στους υπάρχοντες και τους εμφανιζόμενους κινδύνους και τις απειλές, μεταξύ άλλων σε σχέση με τις νέες και αναδυόμενες τεχνολογίες της πληροφορίας και των τηλεπικοινωνιών, και για την αποτελεσματική χρήση τεχνολογιών πρόληψης κινδύνων·

β) συμμετέχει, εφόσον του έχουν ανατεθεί οι συναφείς εξουσίες από την Επιτροπή, στη φάση υλοποίησης των προγραμμάτων χρηματοδότησης της έρευνας και της καινοτομίας ή ως δικαιούχος.

Άρθρο 11
Καθήκοντα σχετικά με τη διεθνή συνεργασία

Ο Οργανισμός συμβάλλει στις προσπάθειες της Ένωσης για συνεργασία της με τρίτες χώρες και διεθνείς οργανισμούς, για την προώθηση της διεθνούς συνεργασίας σε θέματα που αφορούν την ασφάλεια στον κυβερνοχώρο:

α) συμμετέχοντας, όπου είναι σκόπιμο, ως παρατηρητής σε οργανωτικό επίπεδο στην οργάνωση διεθνών ασκήσεων, αναλύοντας τα αποτελέσματά τους και υποβάλλοντας σχετικές εκθέσεις στο διοικητικό συμβούλιο·

β) διευκολύνοντας, κατόπιν αιτήματος της Επιτροπής, την ανταλλαγή βέλτιστων πρακτικών μεταξύ των σχετικών διεθνών οργανισμών·

γ) παρέχοντας, κατόπιν σχετικού αιτήματος, εμπειρογνωσία στην Επιτροπή.

ΚΕΦΑΛΑΙΟ ΙΙ
ΟΡΓΑΝΩΣΗ ΤΟΥ ΟΡΓΑΝΙΣΜΟΥ

Άρθρο 12
Δομή

Η δομή διοίκησης και διαχείρισης του Οργανισμού απαρτίζεται από:

α) το διοικητικό συμβούλιο, το οποίο ασκεί τις αρμοδιότητες που αναφέρονται στο άρθρο 14·

β) το εκτελεστικό συμβούλιο, το οποίο ασκεί τις αρμοδιότητες που καθορίζονται στο άρθρο 18·

γ) τον εκτελεστικό διευθυντή, ο οποίος ασκεί τις αρμοδιότητες που αναφέρονται στο άρθρο 19· και

δ) τη μόνιμη ομάδα ενδιαφερομένων, η οποία ασκεί τις αρμοδιότητες που καθορίζονται στο άρθρο 20.

ΤΜΗΜΑ 1
ΔΙΟΙΚΗΤΙΚΟ ΣΥΜΒΟΥΛΙΟ

Άρθρο 13
Σύνθεση του διοικητικού συμβουλίου

1. Το διοικητικό συμβούλιο απαρτίζεται από έναν εκπρόσωπο από κάθε κράτος μέλος, και δύο εκπρόσωπους που διορίζονται από την Επιτροπή. Όλοι οι εκπρόσωποι έχουν δικαίωμα ψήφου.
2. Για όλα τα μέλη του διοικητικού συμβουλίου προβλέπονται αναπληρωματικά μέλη, που τα εκπροσωπούν σε περίπτωση απουσίας τους.

3. Τα τακτικά και τα αναπληρωματικά μέλη του διοικητικού συμβουλίου διορίζονται με κριτήριο τη γνώση τους στον τομέα της ασφάλειας στον κυβερνοχώρο, ενώ λαμβάνονται επίσης υπόψη οι σχετικές δεξιότητές τους στους τομείς της διαχείρισης, της διοίκησης και του προϋπολογισμού. Η Επιτροπή και τα κράτη μέλη καταβάλλουν προσπάθειες για να περιορίσουν την εναλλαγή των εκπροσώπων τους στο διοικητικό συμβούλιο, προκειμένου να εξασφαλίζεται η συνέχεια του έργου των συμβουλίων. Η Επιτροπή και τα κράτη μέλη επιδιώκουν την ισόρροπη εκπροσώπηση ανδρών και γυναικών στο διοικητικό συμβούλιο.

4. Η θητεία των τακτικών και των αναπληρωματικών μελών του διοικητικού συμβουλίου είναι τετραετής. Η θητεία αυτή είναι ανανεώσιμη.

Άρθρο 14
Καθήκοντα του διοικητικού συμβουλίου

1. Το διοικητικό συμβούλιο:

α) ορίζει τις γενικές κατευθύνσεις λειτουργίας του Οργανισμού και διασφαλίζει επίσης ότι ο Οργανισμός λειτουργεί σύμφωνα με τους κανόνες και τις αρχές που θεσπίστηκαν στον παρόντα κανονισμό. Επίσης, διασφαλίζει τη συνοχή των εργασιών του Οργανισμού με τις δραστηριότητες που διεξάγονται από τα κράτη μέλη, καθώς και σε επίπεδο Ένωσης·

β) εγκρίνει το σχέδιο ενιαίου εγγράφου προγραμματισμού του Οργανισμού που αναφέρεται στο άρθρο 21, πριν από την υποβολή του στην Επιτροπή προκειμένου αυτή να γνωμοδοτήσει σχετικά·

γ) εγκρίνει, λαμβάνοντας υπόψη τη γνώμη της Επιτροπής, το ενιαίο έγγραφο προγραμματισμού του Οργανισμού με πλειοψηφία των δύο τρίτων των μελών του και σύμφωνα με το άρθρο 17·

δ) εγκρίνει, με πλειοψηφία των δύο τρίτων των μελών του, τον ετήσιο προϋπολογισμό του Οργανισμού και ασκεί άλλες αρμοδιότητες σε σχέση με τον προϋπολογισμό του Οργανισμού, σύμφωνα με το κεφάλαιο ΙΙΙ·

ε) αξιολογεί και εγκρίνει την ενοποιημένη ετήσια έκθεση δραστηριοτήτων του Οργανισμού και διαβιβάζει την έκθεση και την αξιολόγησή του, έως την 1η Ιουλίου του επόμενου έτους, στο Ευρωπαϊκό Κοινοβούλιο, στο Συμβούλιο, στην Επιτροπή και στο Ελεγκτικό Συνέδριο. Η ετήσια έκθεση περιλαμβάνει τους λογαριασμούς και περιγράφει με ποιο τρόπο ο Οργανισμός έχει επιτύχει τους δείκτες επιδόσεών του. Η ετήσια έκθεση δημοσιοποιείται·

στ) θεσπίζει τους δημοσιονομικούς κανόνες που εφαρμόζονται στον Οργανισμό σύμφωνα με το άρθρο 29·

ζ) χαράσσει στρατηγική καταπολέμησης της απάτης ανάλογη των κινδύνων απάτης και λαμβάνοντας υπόψη την ανάλυση κόστους-οφέλους των λαμβανόμενων μέτρων·

η) θεσπίζει κανόνες για την πρόληψη και τη διαχείριση συγκρούσεων συμφερόντων στις οποίες εμπλέκονται τα μέλη του·

θ) εξασφαλίζει ότι δίνεται κατάλληλη συνέχεια στα πορίσματα και τις συστάσεις που προκύπτουν από τις έρευνες της Ευρωπαϊκής Υπηρεσίας Καταπολέμησης της Απάτης (OLAF) και τις διάφορες διεθνείς ή εξωτερικές εκθέσεις ελέγχου και αξιολογήσεις·

ι) θεσπίζει τον εσωτερικό του κανονισμό·

ια) ασκεί, σύμφωνα με την παράγραφο 2, όσον αφορά το προσωπικό του Οργανισμού, τις εξουσίες που ανατίθενται από τον κανονισμό υπηρεσιακής κατάστασης των υπαλλήλων στην αρμόδια για τους διορισμούς αρχή και από το καθεστώς που εφαρμόζεται στο λοιπό προσωπικό της Ευρωπαϊκής Ένωσης στην αρχή που είναι επιφορτισμένη με τη σύναψη των συμβάσεων προσλήψεως («εξουσίες αρμόδιας για τους διορισμούς αρχής»)·

ιβ) εγκρίνει κανόνες για την εφαρμογή του κανονισμού υπηρεσιακής κατάστασης και του καθεστώτος που εφαρμόζεται στο λοιπό προσωπικό, σύμφωνα με τη διαδικασία που προβλέπεται στο άρθρο 110 του κανονισμού υπηρεσιακής κατάστασης·

ιγ) διορίζει τον εκτελεστικό διευθυντή και, ανάλογα με την περίπτωση, παρατείνει τη θητεία του ή τον παύει σύμφωνα με το άρθρο 33 του παρόντος κανονισμού·

ιδ) διορίζει υπόλογο, ο οποίος μπορεί να είναι ο υπόλογος της Επιτροπής και ο οποίος λειτουργεί υπό καθεστώς πλήρους ανεξαρτησίας κατά την άσκηση των καθηκόντων του·

ιε) λαμβάνει όλες τις αποφάσεις σχετικά με τη συγκρότηση των εσωτερικών δομών του Οργανισμού και, όπου απαιτείται, σχετικά με την τροποποίησή τους, συνεκτιμώντας τις ανάγκες δραστηριοτήτων του Οργανισμού καθώς και τη χρηστή δημοσιονομική διαχείριση·

ιστ) εγκρίνει τη σύναψη συμφωνιών συνεργασίας σύμφωνα με τα άρθρα 7 και 39.

2. Το διοικητικό συμβούλιο εκδίδει, σύμφωνα με το άρθρο 110 του κανονισμού υπηρεσιακής κατάστασης, απόφαση με βάση το άρθρο 2 παράγραφος 1 του κανονισμού υπηρεσιακής κατάστασης και το άρθρο 6 του καθεστώτος που εφαρμόζεται στο λοιπό προσωπικό, για τη μεταβίβαση των σχετικών εξουσιών αρμόδιας για τους διορισμούς αρχής στον εκτελεστικό διευθυντή, καθώς και για τον προσδιορισμό των προϋποθέσεων με βάση τις οποίες μπορεί να ανασταλεί η εν λόγω μεταβίβαση. Ο εκτελεστικός διευθυντής έχει το δικαίωμα να μεταβιβάζει περαιτέρω τις εν λόγω εξουσίες.

3. Όταν το επιβάλλουν εξαιρετικές περιστάσεις, το διοικητικό συμβούλιο δύναται, με απόφασή του, να αναστείλει προσωρινά τη μεταβίβαση στον εκτελεστικό διευθυντή των εξουσιών αρμόδιας για τους διορισμούς αρχής και των εξουσιών που ο τελευταίος μεταβίβασε περαιτέρω, και να τις ασκήσει το ίδιο ή να τις αναθέσει σε ένα από τα μέλη του ή σε άλλο μέλος του προσωπικού πλην του εκτελεστικού διευθυντή.

Άρθρο 15

Πρόεδρος του διοικητικού συμβουλίου

Το διοικητικό συμβούλιο εκλέγει με πλειοψηφία των δύο τρίτων των μελών του πρόεδρο και αναπληρωτή πρόεδρο μεταξύ των μελών του για θητεία τεσσάρων ετών, η οποία μπορεί να ανανεωθεί μία φορά. Ωστόσο, εάν απολέσουν την ιδιότητα του μέλους του διοικητικού συμβουλίου σε οποιαδήποτε στιγμή της θητείας τους, η θητεία τους λήγει την ίδια ημερομηνία αυτομάτως. Ο αναπληρωτής πρόεδρος αντικαθιστά ex officio τον πρόεδρο, εάν ο τελευταίος δεν είναι σε θέση να εκτελέσει τα καθήκοντά του.

Άρθρο 16

Συνεδριάσεις του διοικητικού συμβουλίου

1. Το διοικητικό συμβούλιο συγκαλείται από τον πρόεδρό του.
2. Το διοικητικό συμβούλιο συνέρχεται σε τακτική συνεδρίαση τουλάχιστον δύο φορές ετησίως. Συνέρχεται επίσης σε έκτακτες συνεδριάσεις με πρωτοβουλία του προέδρου, κατ' αίτηση της Επιτροπής ή κατ' αίτηση τουλάχιστον ενός τρίτου των μελών του.
3. Ο εκτελεστικός διευθυντής συμμετέχει χωρίς δικαίωμα ψήφου στις συνεδριάσεις του διοικητικού συμβουλίου.
4. Τα μέλη της μόνιμης ομάδας ενδιαφερομένων μπορούν να συμμετέχουν, κατόπιν πρόσκλησης από τον πρόεδρο, στις συνεδριάσεις του διοικητικού συμβουλίου, χωρίς δικαίωμα ψήφου.
5. Τα τακτικά και τα αναπληρωματικά μέλη του διοικητικού συμβουλίου, σύμφωνα με τον εσωτερικό του κανονισμό, δύνανται να επικουρούνται στις συνεδριάσεις από συμβούλους ή εμπειρογνώμονες.
6. Ο Οργανισμός παρέχει γραμματειακή υποστήριξη στο διοικητικό συμβούλιο.

Άρθρο 17

Κανόνες ψηφοφορίας του διοικητικού συμβουλίου

1. Το διοικητικό συμβούλιο αποφασίζει με πλειοψηφία των μελών του.
2. Απαιτείται πλειοψηφία δύο τρίτων όλων των μελών του διοικητικού συμβουλίου για την έγκριση του ενιαίου εγγράφου προγραμματισμού και του ετήσιου προϋπολογισμού, καθώς και για τον διορισμό, την παράταση της θητείας και την παύση του εκτελεστικού διευθυντή.
3. Κάθε μέλος διαθέτει μία ψήφο. Κατά την απουσία μέλους, το δικαίωμα ψήφου του δικαιούται να ασκήσει ο αναπληρωτής του.
4. Ο πρόεδρος συμμετέχει στην ψηφοφορία.
5. Ο εκτελεστικός διευθυντής δεν συμμετέχει στην ψηφοφορία.
6. Λεπτομερέστερες ρυθμίσεις σχετικά με την ψηφοφορία, ιδίως όσον αφορά τις προϋποθέσεις υπό τις οποίες ένα μέλος μπορεί να ενεργεί εξ ονόματος άλλου μέλους, καθορίζονται στον εσωτερικό κανονισμό του διοικητικού συμβουλίου.

ΤΜΗΜΑ 2
ΕΚΤΕΛΕΣΤΙΚΟ ΣΥΜΒΟΥΛΙΟ

Άρθρο 18
Εκτελεστικό συμβούλιο

1. Το διοικητικό συμβούλιο επικουρείται από το εκτελεστικό συμβούλιο.

2. Το εκτελεστικό συμβούλιο:

   α) προετοιμάζει τις αποφάσεις που λαμβάνει το διοικητικό συμβούλιο·

   β) εξασφαλίζει, μαζί με το διοικητικό συμβούλιο, την κατάλληλη συνέχεια στα πορίσματα και τις συστάσεις που προκύπτουν από τις έρευνες της OLAF και τις διάφορες διεθνείς ή εξωτερικές εκθέσεις ελέγχου και αξιολογήσεις·

   γ) με την επιφύλαξη των αρμοδιοτήτων του εκτελεστικού διευθυντή, όπως καθορίζονται στο άρθρο 19, επικουρεί και συμβουλεύει τον εκτελεστικό διευθυντή όσον αφορά την εκτέλεση των αποφάσεων του διοικητικού συμβουλίου για διοικητικά και δημοσιονομικά θέματα σύμφωνα με το άρθρο 19.

3. Το εκτελεστικό συμβούλιο απαρτίζεται από πέντε μέλη, που επιλέγονται μεταξύ των μελών του διοικητικού συμβουλίου, και στα οποία συγκαταλέγονται ο πρόεδρος του διοικητικού συμβουλίου, που μπορεί να ασκεί και την προεδρία του εκτελεστικού συμβουλίου, και ένας από τους εκπροσώπους της Επιτροπής. Ο εκτελεστικός διευθυντής συμμετέχει στις συνεδριάσεις του εκτελεστικού συμβουλίου χωρίς δικαίωμα ψήφου.

4. Η διάρκεια της θητείας των μελών του εκτελεστικού συμβουλίου είναι τετραετής. Η θητεία αυτή είναι ανανεώσιμη.

5. Το εκτελεστικό συμβούλιο συνέρχεται τουλάχιστον μια φορά το τρίμηνο. Ο πρόεδρος του εκτελεστικού συμβουλίου συγκαλεί έκτακτες συνεδριάσεις μετά από αίτημα των μελών του.

6. Το διοικητικό συμβούλιο θεσπίζει τον εσωτερικό κανονισμό του εκτελεστικού συμβουλίου.

7. Όταν καθίσταται απαραίτητο, λόγω έκτακτης ανάγκης, το εκτελεστικό συμβούλιο δύναται να λάβει ορισμένες προσωρινές αποφάσεις εξ ονόματος του διοικητικού συμβουλίου, ιδίως σε θέματα διοικητικής διαχείρισης, συμπεριλαμβανομένης της αναστολής της μεταβίβασης εξουσιών αρμόδιας για τους διορισμούς αρχής, καθώς και σε θέματα προϋπολογισμού.

ΤΜΗΜΑ 3
ΕΚΤΕΛΕΣΤΙΚΟΣ ΔΙΕΥΘΥΝΤΗΣ

Άρθρο 19
Αρμοδιότητες του εκτελεστικού διευθυντή

1. Ο Οργανισμός διοικείται από τον εκτελεστικό διευθυντή του, ο οποίος ενεργεί ανεξάρτητα κατά την άσκηση των καθηκόντων του. Ο εκτελεστικός διευθυντής λογοδοτεί στο διοικητικό συμβούλιο.

2. Ο εκτελεστικός διευθυντής υποβάλλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο σχετικά με την εκτέλεση των καθηκόντων του κατόπιν σχετικού αιτήματος. Το Συμβούλιο μπορεί να καλέσει τον εκτελεστικό διευθυντή να υποβάλει έκθεση σχετικά με την εκτέλεση των καθηκόντων του.

3. Ο εκτελεστικός διευθυντής είναι υπεύθυνος για:

α) την τρέχουσα διοίκηση του Οργανισμού·

β) την εκτέλεση των αποφάσεων που έχουν εγκριθεί από το διοικητικό συμβούλιο·

γ) την εκπόνηση του σχεδίου ενιαίου εγγράφου προγραμματισμού και την υποβολή του στο διοικητικό συμβούλιο προς έγκριση, πριν από την υποβολή του στην Επιτροπή·

δ) την εφαρμογή του ενιαίου εγγράφου προγραμματισμού και την υποβολή σχετικής έκθεσης στο διοικητικό συμβούλιο·

ε) την κατάρτιση της ενοποιημένης ετήσιας έκθεσης δραστηριοτήτων του Οργανισμού και την υποβολή της στο διοικητικό συμβούλιο προς αξιολόγηση και έγκριση·

στ) την κατάρτιση σχεδίου δράσης για να δοθεί συνέχεια στα συμπεράσματα των αναδρομικών αξιολογήσεων και την υποβολή έκθεσης προόδου στην Επιτροπή ανά δύο έτη·

ζ) την κατάρτιση σχεδίου δράσης με βάση τα πορίσματα εσωτερικών ή εξωτερικών εκθέσεων ελέγχου, καθώς και ερευνών της Ευρωπαϊκής Υπηρεσίας Καταπολέμησης της Απάτης (OLAF) και την υποβολή έκθεσης προόδου δύο φορές ετησίως στην Επιτροπή και ανά τακτά χρονικά διαστήματα στο διοικητικό συμβούλιο·

η) την εκπόνηση σχεδίου των δημοσιονομικών κανόνων που εφαρμόζονται στον Οργανισμό·

θ) την κατάρτιση του σχεδίου κατάστασης προβλεπόμενων εσόδων και εξόδων του Οργανισμού και την εκτέλεση του προϋπολογισμού του·

ι) την προστασία των οικονομικών συμφερόντων της Ένωσης, με την εφαρμογή προληπτικών μέτρων κατά της απάτης, της διαφθοράς και άλλων παράνομων δραστηριοτήτων, με αποτελεσματικούς ελέγχους και, σε περίπτωση που διαπιστωθούν παρατυπίες, με την ανάκτηση των αχρεωστήτως καταβληθέντων ποσών και, όπου είναι σκόπιμο, την επιβολή αποτελεσματικών, αναλογικών και αποτρεπτικών διοικητικών και οικονομικών κυρώσεων·

ια) τη χάραξη στρατηγικής του Οργανισμού, για την καταπολέμηση της απάτης, και την υποβολή της στο διοικητικό συμβούλιο προς έγκριση·

ιβ) την ανάπτυξη και διατήρηση επαφών με την επιχειρηματική κοινότητα και τις ενώσεις καταναλωτών, ώστε να εξασφαλίζεται τακτικός διάλογος με τους σχετικούς άμεσα ενδιαφερομένους·

ιγ) άλλα καθήκοντα που ανατίθενται στον εκτελεστικό διευθυντή δυνάμει του παρόντος κανονισμού.

4. Εφόσον κρίνεται αναγκαίο, και στο πλαίσιο της εντολής του Οργανισμού και σύμφωνα με τους στόχους και τα καθήκοντα του Οργανισμού, ο εκτελεστικός διευθυντής μπορεί να συγκροτεί ad hoc ομάδες εργασίας οι οποίες απαρτίζονται από εμπειρογνώμονες, μεταξύ άλλων από τις αρμόδιες αρχές των κρατών μελών. Το διοικητικό συμβούλιο ενημερώνεται εκ των προτέρων. Οι διαδικασίες, ιδίως όσον αφορά τη σύνθεση των ομάδων εργασίας, τον διορισμό των εμπειρογνωμόνων των ομάδων εργασίας από τον εκτελεστικό διευθυντή και τη λειτουργία των ομάδων εργασίας, προσδιορίζονται στους εσωτερικούς κανόνες λειτουργίας του Οργανισμού.

5. Ο εκτελεστικός διευθυντής αποφασίζει αν είναι αναγκαίο να τοποθετηθούν υπάλληλοι σε ένα ή περισσότερα κράτη μέλη για την αποτελεσματική και επαρκή άσκηση των καθηκόντων του Οργανισμού. Προτού λάβει απόφαση για εγκαθίδρυση τοπικού γραφείου, ο εκτελεστικός διευθυντής λαμβάνει εκ των προτέρων τη συγκατάθεση της Επιτροπής, του διοικητικού συμβουλίου και του οικείου κράτους μέλους ή κρατών μελών. Στην απόφαση διευκρινίζεται το πεδίο εφαρμογής των δραστηριοτήτων που πρόκειται να αναλάβει το τοπικό γραφείο, ώστε να αποφεύγεται το αδικαιολόγητο κόστος και η επικάλυψη διοικητικών καθηκόντων του Οργανισμού. Συμφωνία με το/τα οικείο/-α κράτος/-η μέλος/-η επιτυγχάνεται εφόσον κρίνεται σκόπιμο ή αναγκαίο.

ΤΜΗΜΑ 4
ΜΟΝΙΜΗ ΟΜΑΔΑ ΕΝΔΙΑΦΕΡΟΜΕΝΩΝ

Άρθρο 20
Μόνιμη ομάδα ενδιαφερομένων

1. Το διοικητικό συμβούλιο, κατόπιν προτάσεως του εκτελεστικού διευθυντή, συγκροτεί μια μόνιμη ομάδα ενδιαφερομένων η οποία απαρτίζεται από εμπειρογνώμονες αναγνωρισμένου κύρους που αντιπροσωπεύουν τους σχετικούς άμεσα ενδιαφερομένους, όπως τον κλάδο ΤΠΕ, τους παρόχους δικτύων ή υπηρεσιών ηλεκτρονικών επικοινωνιών για το κοινό, τις ομάδες καταναλωτών, τους πανεπιστημιακούς που είναι ειδικοί στην ασφάλεια στον κυβερνοχώρο, και αντιπροσώπους των αρμόδιων αρχών στις οποίες υποβάλλεται κοινοποίηση σύμφωνα με την [οδηγία για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών], όπως επίσης και των αρχών επιβολής του νόμου και των εποπτικών αρχών προστασίας δεδομένων.

2. Οι διαδικασίες της μόνιμης ομάδας ενδιαφερομένων, ιδίως όσον αφορά τον αριθμό, τη σύνθεση και τον διορισμό των μελών της από το διοικητικό συμβούλιο, την πρόταση του εκτελεστικού διευθυντή, καθώς και τη λειτουργία της ομάδας, καθορίζονται στους εσωτερικούς κανόνες λειτουργίας του Οργανισμού και δημοσιοποιούνται.

3. Πρόεδρος της μόνιμης ομάδας ενδιαφερομένων είναι ο εκτελεστικός διευθυντής ή πρόσωπο διορισμένο από τον εκτελεστικό διευθυντή, κατά περίπτωση.

4. Η διάρκεια της θητείας των μελών της μόνιμης ομάδας ενδιαφερομένων είναι δυόμισι έτη. Τα μέλη του διοικητικού συμβουλίου δεν επιτρέπεται να είναι μέλη της μόνιμης ομάδας ενδιαφερομένων. Οι εμπειρογνώμονες της Επιτροπής και των κρατών μελών έχουν δικαίωμα να παρίστανται στις συνεδριάσεις της μόνιμης ομάδας ενδιαφερομένων και να συμμετέχουν στις εργασίες της. Μπορούν να προσκαλούνται να παρίστανται σε συνεδριάσεις της μόνιμης ομάδας ενδιαφερομένων και να συμμετέχουν στις εργασίες της εκπρόσωποι άλλων φορέων που δεν είναι μέλη της, αν το κρίνει σκόπιμο ο εκτελεστικός διευθυντής.

5. Η μόνιμη ομάδα ενδιαφερομένων παρέχει συμβουλές στον Οργανισμό σχετικά με την εκτέλεση των δραστηριοτήτων του. Παρέχει συμβουλές ειδικότερα στον εκτελεστικό διευθυντή κατά την κατάρτιση πρότασης για το πρόγραμμα εργασίας του Οργανισμού και για τη διασφάλιση της επικοινωνίας με τους σχετικούς άμεσα ενδιαφερομένους επί όλων των θεμάτων που σχετίζονται με το πρόγραμμα εργασίας.

ΤΜΗΜΑ 5
ΛΕΙΤΟΥΡΓΙΑ

Άρθρο 21
Ενιαίο έγγραφο προγραμματισμού

1. Ο Οργανισμός εκτελεί τις εργασίες του σύμφωνα με το ενιαίο έγγραφο προγραμματισμού που περιέχει το πολυετές και ετήσιο πρόγραμμά του και περιλαμβάνει όλες τις προγραμματισμένες δραστηριότητές του.

2. Κάθε χρόνο, ο εκτελεστικός διευθυντής συντάσσει σχέδιο ενιαίου εγγράφου προγραμματισμού που περιέχει πολυετές και ετήσιο πρόγραμμα με τον αντίστοιχο προγραμματισμό των ανθρώπινων και οικονομικών πόρων, σύμφωνα με το άρθρο 32 του κατ' εξουσιοδότηση κανονισμού (ΕΕ) αριθ. 1271/2013 της Επιτροπής[36] και λαμβάνοντας υπόψη τις κατευθυντήριες γραμμές της Επιτροπής.

3. Έως τις 30 Νοεμβρίου κάθε έτους, το διοικητικό συμβούλιο εγκρίνει το ενιαίο έγγραφο προγραμματισμού που αναφέρεται στην παράγραφο 1 και το διαβιβάζει στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και την Επιτροπή το αργότερο έως τις 31 Ιανουαρίου του επόμενου έτους, καθώς και κάθε μεταγενέστερη επικαιροποιημένη έκδοση του εγγράφου αυτού.

4. Το ενιαίο έγγραφο προγραμματισμού οριστικοποιείται μετά την τελική έγκριση του γενικού προϋπολογισμού της Ένωσης και, εάν χρειαστεί, προσαρμόζεται ανάλογα.

5. Το ετήσιο πρόγραμμα εργασίας περιλαμβάνει λεπτομερείς στόχους και αναμενόμενα αποτελέσματα, καθώς και δείκτες επιδόσεων. Περιλαμβάνει επίσης περιγραφή των προς χρηματοδότηση δράσεων και αναφέρει τους οικονομικούς και ανθρώπινους πόρους που διατίθενται για κάθε δράση, σύμφωνα με τις αρχές κατάρτισης και διαχείρισης του προϋπολογισμού βάσει δραστηριοτήτων. Το ετήσιο πρόγραμμα εργασίας συνάδει με το πολυετές πρόγραμμα εργασίας που αναφέρεται στην

---

36 Κατ' εξουσιοδότηση κανονισμός (ΕΕ) αριθ. 1271/2013 της Επιτροπής, της 30ής Σεπτεμβρίου 2013, για τη θέσπιση του δημοσιονομικού κανονισμού-πλαισίου για τους οργανισμούς που αναφέρονται στο άρθρο 208 του κανονισμού (ΕΕ, Ευρατόμ) αριθ. 966/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (ΕΕ L 328 της 7.12.2013, σ. 42)

παράγραφο 7. Αναφέρει σαφώς τα καθήκοντα που έχουν προστεθεί, μεταβληθεί ή απαλειφθεί σε σχέση με το προηγούμενο οικονομικό έτος.

6. Όταν ανατίθεται στον Οργανισμό νέο καθήκον, το διοικητικό συμβούλιο τροποποιεί το εγκεκριμένο ετήσιο πρόγραμμα εργασίας. Κάθε ουσιώδης τροποποίηση του ετήσιου προγράμματος εργασίας εγκρίνεται με την ίδια διαδικασία που εφαρμόζεται και στο αρχικό ετήσιο πρόγραμμα εργασίας. Το διοικητικό συμβούλιο μπορεί να εξουσιοδοτεί τον εκτελεστικό διευθυντή να επιφέρει μη ουσιώδεις τροποποιήσεις στο ετήσιο πρόγραμμα εργασίας.

7. Το πολυετές πρόγραμμα εργασίας καθορίζει τον συνολικό στρατηγικό προγραμματισμό που περιλαμβάνει στόχους, αναμενόμενα αποτελέσματα και δείκτες επιδόσεων. Καθορίζει επίσης τον προγραμματισμό των πόρων, που περιλαμβάνει τον πολυετή προϋπολογισμό και το προσωπικό.

8. Ο προγραμματισμός των πόρων επικαιροποιείται σε ετήσια βάση. Ο στρατηγικός προγραμματισμός επικαιροποιείται κατά περίπτωση, και ιδίως εφόσον κρίνεται αναγκαίο για αντιμετώπιση θεμάτων που προκύπτουν από την αξιολόγηση που αναφέρεται στο άρθρο 56.

Άρθρο 22
Δήλωση συμφερόντων

1. Τα μέλη του διοικητικού συμβουλίου, ο εκτελεστικός διευθυντής και οι υπάλληλοι που αποσπώνται προσωρινά από τα κράτη μέλη υποβάλλουν έκαστος δήλωση δεσμεύσεων και γραπτή δήλωση συμφερόντων όπου καταδεικνύεται η απουσία ή ύπαρξη οποιουδήποτε άμεσου ή έμμεσου συμφέροντος που θα μπορούσε να επηρεάσει την ανεξαρτησία τους. Οι δηλώσεις είναι ακριβείς και πλήρεις, υποβάλλονται σε ετήσια βάση εγγράφως, και ενημερώνονται όποτε είναι αναγκαίο.

2. Τα μέλη του διοικητικού συμβουλίου, ο εκτελεστικός διευθυντής και οι εξωτερικοί εμπειρογνώμονες, οι οποίοι συμμετέχουν στις ad hoc ομάδες εργασίας δηλώνουν έκαστος με ακρίβεια και πληρότητα το αργότερο στην έναρξη κάθε συνεδρίασης οιαδήποτε συμφέροντα τα οποία μπορούν ενδεχομένως να επηρεάσουν την ανεξαρτησία τους σε σχέση με τα θέματα της ημερήσιας διάταξης και δεν συμμετέχουν στη συζήτηση και την ψηφοφορία των εν λόγω θεμάτων.

3. Ο Οργανισμός θεσπίζει στους εσωτερικούς κανόνες λειτουργίας του τα πρακτικά μέτρα εφαρμογής των κανόνων για τις δηλώσεις συμφερόντων που αναφέρονται στις παραγράφους 1 και 2.

Άρθρο 23
Διαφάνεια

1. Ο Οργανισμός διεξάγει τις δραστηριότητές του με υψηλό επίπεδο διαφάνειας και σύμφωνα με το άρθρο 25.

2. Ο Οργανισμός μεριμνά ώστε να παρέχονται στο κοινό και σε κάθε ενδιαφερόμενο μέρος οι ενδεδειγμένες αντικειμενικές, αξιόπιστες και εύκολα προσβάσιμες πληροφορίες, ιδίως όσον αφορά τα αποτελέσματα των εργασιών του. Ο Οργανισμός δημοσιοποιεί επίσης τις δηλώσεις συμφερόντων που υποβάλλονται δυνάμει του άρθρου 22.

3. Το διοικητικό συμβούλιο, ενεργώντας κατόπιν προτάσεως του εκτελεστικού διευθυντή, μπορεί να επιτρέπει στα ενδιαφερόμενα μέρη να συμμετέχουν ως παρατηρητές σε ορισμένες δραστηριότητες του Οργανισμού.

4. Ο Οργανισμός θεσπίζει, στους εσωτερικούς κανόνες λειτουργίας του, τα πρακτικά μέτρα εφαρμογής των κανόνων διαφάνειας που αναφέρονται στις παραγράφους 1 και 2.

Άρθρο 24
Τήρηση απορρήτου

1. Με την επιφύλαξη του άρθρου 25, ο Οργανισμός δεν αποκαλύπτει σε τρίτους πληροφορίες που επεξεργάζεται ή λαμβάνει και σχετικά με τις οποίες έχει υποβληθεί τεκμηριωμένο αίτημα για πλήρη ή μερική τήρηση του απορρήτου.

2. Τα μέλη του διοικητικού συμβουλίου, ο εκτελεστικός διευθυντής, τα μέλη της μόνιμης ομάδας ενδιαφερομένων, οι εξωτερικοί εμπειρογνώμονες που συμμετέχουν στις ad hoc ομάδες εργασίας, καθώς και τα μέλη του προσωπικού του Οργανισμού, συμπεριλαμβανομένων των υπαλλήλων που αποσπώνται προσωρινά από τα κράτη μέλη, συμμορφώνονται, ακόμη και μετά την παύση των καθηκόντων τους, στις απαιτήσεις τήρησης του απορρήτου, σύμφωνα με το άρθρο 339 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ).

3. Ο Οργανισμός θεσπίζει, στους εσωτερικούς κανόνες λειτουργίας του, τα πρακτικά μέτρα εφαρμογής των κανόνων περί απορρήτου που προβλέπονται στις παραγράφους 1 και 2.

4. Αν απαιτείται για την επιτέλεση των καθηκόντων του Οργανισμού, το διοικητικό συμβούλιο αποφασίζει να επιτρέψει στον Οργανισμό να χειρίζεται διαβαθμισμένες πληροφορίες. Σε αυτή την περίπτωση, το διοικητικό συμβούλιο, κατόπιν συμφωνίας με τις υπηρεσίες της Επιτροπής, εγκρίνει τους εσωτερικούς κανόνες λειτουργίας του εφαρμόζοντας τις αρχές ασφαλείας που ορίζονται στην απόφαση (ΕΚ, Ευρατόμ) 2015/443 της Επιτροπής[37] και στην απόφαση (ΕΚ, Ευρατόμ) 2015/444 της Επιτροπής[38]. Οι κανόνες αυτοί περιλαμβάνουν διατάξεις που έχουν σχέση με την ανταλλαγή, την επεξεργασία και την αποθήκευση διαβαθμισμένων πληροφοριών.

Άρθρο 25
Πρόσβαση σε έγγραφα

1. Ο κανονισμός (ΕΚ) αριθ. 1049/2001 εφαρμόζεται για τα έγγραφα που τηρεί ο Οργανισμός.

2. Το διοικητικό συμβούλιο εγκρίνει διατάξεις για την εφαρμογή του κανονισμού (ΕΚ) αριθ. 1049/2001 εντός έξι μηνών από την ίδρυση του Οργανισμού.

3. Οι αποφάσεις που λαμβάνονται από τον Οργανισμό σύμφωνα με το άρθρο 8 του κανονισμού (ΕΚ) αριθ. 1049/2001 είναι δυνατόν να αποτελέσουν αντικείμενο καταγγελίας στον Διαμεσολαβητή σύμφωνα με το άρθρο 228 ΣΛΕΕ ή προσφυγής ενώπιον του Δικαστηρίου της Ευρωπαϊκής Ένωσης σύμφωνα με το άρθρο 263 ΣΛΕΕ.

---

37 Απόφαση (ΕΚ, Ευρατόμ) 2015/443 της Επιτροπής, της 13ης Μαρτίου 2015, σχετικά με την ασφάλεια στην Επιτροπή (ΕΕ L 72 της 17.3.2015, σ. 41).

38 Απόφαση (ΕΚ, Ευρατόμ) 2015/444 της Επιτροπής, της 13ης Μαρτίου 2015, σχετικά με τους κανόνες ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών της ΕΕ (ΕΕ L 72 της 17.3.2015, σ. 53).

ΚΕΦΑΛΑΙΟ ΙΙΙ
ΚΑΤΑΡΤΙΣΗ ΚΑΙ ΔΙΑΡΘΡΩΣΗ ΤΟΥ ΠΡΟΫΠΟΛΟΓΙΣΜΟΥ

Άρθρο 26
Κατάρτιση του προϋπολογισμού

1. Κάθε έτος, ο εκτελεστικός διευθυντής καταρτίζει σχέδιο κατάστασης προβλεπόμενων εσόδων και εξόδων του Οργανισμού για το επόμενο οικονομικό έτος και το διαβιβάζει στο διοικητικό συμβούλιο, μαζί με σχέδιο πίνακα προσωπικού. Τα έσοδα και τα έξοδα ισοσκελίζονται.

2. Κάθε έτος, το διοικητικό συμβούλιο καταρτίζει, βάσει του σχεδίου κατάστασης προβλεπόμενων εσόδων και εξόδων που αναφέρεται στην παράγραφο 1, την κατάσταση προβλεπόμενων εσόδων και εξόδων του Οργανισμού για το επόμενο οικονομικό έτος.

3. Η κατάσταση προβλέψεων που αναφέρεται στην παράγραφο 2, η οποία αποτελεί μέρος του σχεδίου ενιαίου εγγράφου προγραμματισμού, διαβιβάζεται από το διοικητικό συμβούλιο έως την 31η Ιανουαρίου κάθε έτους στην Επιτροπή και στα τρίτα κράτη με τα οποία η Ένωση έχει συνάψει συμφωνίες βάσει του άρθρου 39.

4. Βάσει της εν λόγω κατάστασης προβλέψεων, η Επιτροπή εγγράφει στο σχέδιο του προϋπολογισμού της Ένωσης τις προβλέψεις που κρίνει αναγκαίες για τον πίνακα προσωπικού και το ποσό της συνεισφοράς που θα βαρύνει τον γενικό προϋπολογισμό, και τα υποβάλλει στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο, σύμφωνα με τα άρθρα 313 και 314 ΣΛΕΕ.

5. Το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο εγκρίνουν τις πιστώσεις για τη συνεισφορά στον Οργανισμό.

6. Το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο εγκρίνουν τον πίνακα προσωπικού του Οργανισμού.

7. Παράλληλα με το ενιαίο έγγραφο προγραμματισμού, το διοικητικό συμβούλιο εγκρίνει τον προϋπολογισμό του Οργανισμού. Ο προϋπολογισμός καθίσταται οριστικός μετά την οριστική έγκριση του γενικού προϋπολογισμού της Ένωσης. Εφόσον κρίνεται σκόπιμο, το διοικητικό συμβούλιο προσαρμόζει τον προϋπολογισμό και το ενιαίο έγγραφο προγραμματισμού του Οργανισμού σύμφωνα με τον γενικό προϋπολογισμό της Ένωσης.

Άρθρο 27
Διάρθρωση του προϋπολογισμού

1. Με την επιφύλαξη άλλων πόρων, τα έσοδα του Οργανισμού προέρχονται από:

   α) συνεισφορά από τον προϋπολογισμό της Ένωσης·

   β) έσοδα προοριζόμενα για τη χρηματοδότηση συγκεκριμένων δαπανών, σύμφωνα με τους δημοσιονομικούς κανόνες του που αναφέρονται στο άρθρο 29·

   γ) χρηματοδότηση από την Ένωση υπό μορφή συμφωνιών ανάθεσης ή ad hoc επιδοτήσεων σύμφωνα με τους δημοσιονομικούς κανόνες που αναφέρονται στο άρθρο 29 και τις διατάξεις των συναφών νομικών πράξεων που πλαισιώνουν τις πολιτικές της Ένωσης·

δ) εισφορές τρίτων χωρών που συμμετέχουν στις εργασίες του Οργανισμού όπως προβλέπεται στο άρθρο 39·

ε) τυχόν εθελοντικές εισφορές των κρατών μελών σε χρήματα ή σε είδος. Τα κράτη μέλη που παρέχουν εθελοντικές εισφορές δεν μπορούν να απαιτούν ειδικά δικαιώματα ή υπηρεσίες ως συνέπεια αυτών των εισφορών.

2. Στα έξοδα του Οργανισμού συγκαταλέγονται οι δαπάνες προσωπικού, οι δαπάνες διοικητικής και τεχνικής υποστήριξης, τα έξοδα υποδομής και τα λειτουργικά έξοδα, καθώς και οι δαπάνες για τη σύναψη συμβάσεων με τρίτους.

Άρθρο 28
Εκτέλεση του προϋπολογισμού

1. Ο εκτελεστικός διευθυντής είναι υπεύθυνος για την εκτέλεση του προϋπολογισμού του Οργανισμού.

2. Ο εσωτερικός ελεγκτής της Επιτροπής ασκεί τις ίδιες εξουσίες έναντι του Οργανισμού όπως και έναντι των υπηρεσιών της Επιτροπής.

3. Έως την 1η Μαρτίου μετά τη λήξη κάθε οικονομικού έτους (1η Μαρτίου του έτους N + 1), ο υπόλογος του Οργανισμού διαβιβάζει τους προσωρινούς λογαριασμούς στον υπόλογο της Επιτροπής και στο Ελεγκτικό Συνέδριο.

4. Μετά την παραλαβή των παρατηρήσεων του Ελεγκτικού Συνεδρίου επί των προσωρινών λογαριασμών του Οργανισμού, ο υπόλογος του Οργανισμού καταρτίζει τους οριστικούς λογαριασμούς του Οργανισμού με δική του ευθύνη.

5. Ο εκτελεστικός διευθυντής υποβάλλει τους οριστικούς λογαριασμούς προς γνωμοδότηση στο διοικητικό συμβούλιο.

6. Ο εκτελεστικός διευθυντής διαβιβάζει, έως την 31η Μαρτίου του έτους N + 1, την έκθεση σχετικά με τη δημοσιονομική και χρηματοοικονομική διαχείριση στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Επιτροπή και το Ελεγκτικό Συνέδριο.

7. Έως την 1η Ιουλίου του έτους N + 1, ο υπόλογος διαβιβάζει στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, τον υπόλογο της Επιτροπής και το Ελεγκτικό Συνέδριο τους οριστικούς λογαριασμούς, συνοδευόμενους από τη γνώμη του διοικητικού συμβουλίου.

8. Την ίδια ημέρα που διαβιβάζει τους οριστικούς του λογαριασμούς, ο υπόλογος διαβιβάζει επίσης στο Ελεγκτικό Συνέδριο, με κοινοποίηση στον υπόλογο της Επιτροπής, δήλωση πληρότητας σχετικά με τους οριστικούς αυτούς λογαριασμούς.

9. Ο εκτελεστικός διευθυντής δημοσιεύει τους οριστικούς λογαριασμούς έως τις 15 Νοεμβρίου του επόμενου έτους.

10. Ο εκτελεστικός διευθυντής αποστέλλει στο Ελεγκτικό Συνέδριο απάντηση στις παρατηρήσεις του έως τις 30 Σεπτεμβρίου του έτους N + 1 και αποστέλλει επίσης αντίγραφο της εν λόγω απάντησης στο διοικητικό συμβούλιο και την Επιτροπή.

11. Ο εκτελεστικός διευθυντής υποβάλλει στο Ευρωπαϊκό Κοινοβούλιο, κατόπιν αιτήματος του τελευταίου, κάθε πληροφορία που απαιτείται για την ομαλή εφαρμογή της διαδικασίας απαλλαγής για το συγκεκριμένο οικονομικό έτος, σύμφωνα με το άρθρο 165 παράγραφος 3 του δημοσιονομικού κανονισμού.

12. Έπειτα από σύσταση του Συμβουλίου, το Ευρωπαϊκό Κοινοβούλιο χορηγεί πριν από τις 15 Μαΐου του έτους N + 2 απαλλαγή στον εκτελεστικό διευθυντή για την εκτέλεση του προϋπολογισμού του οικονομικού έτους N.

Άρθρο 29
Δημοσιονομικοί κανόνες

Οι δημοσιονομικοί κανόνες που ισχύουν για τον Οργανισμό θεσπίζονται από το διοικητικό συμβούλιο κατόπιν διαβούλευσης με την Επιτροπή. Οι εν λόγω κανόνες δεν αποκλίνουν από τον κανονισμό (ΕΕ) αριθ. 1271/2013 παρά μόνον εάν το απαιτούν ειδικές ανάγκες λειτουργίας του Οργανισμού και με προηγούμενη συμφωνία της Επιτροπής.

Άρθρο 30
Καταπολέμηση της απάτης

1. Για τη διευκόλυνση της καταπολέμησης της απάτης, της διαφθοράς και άλλων παράνομων πράξεων δυνάμει του κανονισμού (ΕΕ, Ευρατόμ) αριθ. 883/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[39], ο Οργανισμός, μέσα σε διάστημα έξι μηνών από την ημέρα που τέθηκε σε λειτουργία, προσχωρεί στη διοργανική συμφωνία της 25ης Μαΐου 1999 σχετικά με τις εσωτερικές έρευνες που πραγματοποιούνται από την Ευρωπαϊκή Υπηρεσία Καταπολέμησης της Απάτης (OLAF) και θεσπίζει τις ενδεδειγμένες διατάξεις που εφαρμόζονται σε όλους τους υπαλλήλους του Οργανισμού, χρησιμοποιώντας το υπόδειγμα που περιλαμβάνεται στο παράρτημα της εν λόγω συμφωνίας.

2. Το Ελεγκτικό Συνέδριο έχει αρμοδιότητα ελέγχου βάσει παραστατικών και επιτόπιου ελέγχου, η οποία ασκείται σε όλους τους δικαιούχους, εργολάβους και υπεργολάβους που έλαβαν ενωσιακά κονδύλια από τον Οργανισμό.

3. Η OLAF μπορεί να διεξάγει έρευνες, συμπεριλαμβανομένων επιτόπιων ελέγχων και εξακριβώσεων, σύμφωνα με τις διατάξεις και τις διαδικασίες που καθορίζονται στον κανονισμό (ΕΕ, Ευρατόμ) αριθ. 883/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και στον κανονισμό (Ευρατόμ, ΕΚ) αριθ. 2185/96 του Συμβουλίου[40], της 11ης Νοεμβρίου 1996, σχετικά με τους ελέγχους και εξακριβώσεις που διεξάγει επιτοπίως η Επιτροπή με σκοπό την προστασία των οικονομικών συμφερόντων της Ένωσης από απάτες και λοιπές παρατυπίες, για τη διαπίστωση τυχόν απάτης, διαφθοράς ή οποιασδήποτε άλλης παράνομης ενέργειας εις βάρος των οικονομικών συμφερόντων της Ένωσης σε σχέση με χρηματοδότηση που παρέχεται από την Ένωση στο πλαίσιο επιχορήγησης ή σύμβασης χρηματοδοτούμενης από τον Οργανισμό.

4. Με την επιφύλαξη των παραγράφων 1, 2 και 3, οι συμφωνίες συνεργασίας με τρίτες χώρες και με διεθνείς οργανισμούς, οι συμβάσεις, οι συμφωνίες επιχορήγησης και οι αποφάσεις επιχορήγησης του οργανισμού περιέχουν διατάξεις οι οποίες

---

39 Κανονισμός (ΕΕ, Ευρατόμ) αριθ. 883/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Σεπτεμβρίου 2013, σχετικά με τις έρευνες που πραγματοποιούνται από την Ευρωπαϊκή Υπηρεσία Καταπολέμησης της Απάτης (OLAF) και την κατάργηση του κανονισμού (ΕΚ) αριθ. 1073/1999 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και του κανονισμού (Ευρατόμ) αριθ. 1074/1999 του Συμβουλίου (ΕΕ L 248 της18.9.2013, σ. 1).

40 Κανονισμός (Ευρατόμ, ΕΚ) αριθ. 2185/96 του Συμβουλίου, της 11ης Νοεμβρίου 1996, σχετικά με τους ελέγχους και εξακριβώσεις που διεξάγει επιτοπίως η Επιτροπή με σκοπό την προστασία των οικονομικών συμφερόντων των Ευρωπαϊκών Κοινοτήτων από απάτες και λοιπές παρατυπίες (ΕΕ L 292 της 15.11.1996, σ. 2).

εξουσιοδοτούν ρητά το Ελεγκτικό Συνέδριο και την OLAF να διεξάγουν τους εν λόγω λογιστικούς ελέγχους και έρευνες, σύμφωνα με τις αντίστοιχες αρμοδιότητές τους.

ΚΕΦΑΛΑΙΟ IV
ΠΡΟΣΩΠΙΚΟ ΤΟΥ ΟΡΓΑΝΙΣΜΟΥ

Άρθρο 31
Γενικές διατάξεις

Στους υπαλλήλους του Οργανισμού εφαρμόζονται ο κανονισμός υπηρεσιακής κατάστασης και το καθεστώς που εφαρμόζεται στο λοιπό προσωπικό, καθώς και οι εκτελεστικοί κανόνες που θεσπίστηκαν με συμφωνία μεταξύ των θεσμικών οργάνων της Ένωσης για την εφαρμογή του εν λόγω κανονισμού υπηρεσιακής κατάστασης.

Άρθρο 32
Προνόμια και ασυλίες

Το πρωτόκολλο αριθ. 7 περί των προνομίων και ασυλιών της Ευρωπαϊκής Ένωσης το οποίο προσαρτάται στη Συνθήκη για την Ευρωπαϊκή Ένωση και στη ΣΛΕΕ εφαρμόζεται στον Οργανισμό και το προσωπικό του.

Άρθρο 33
Εκτελεστικός διευθυντής

1. Ο εκτελεστικός διευθυντής προσλαμβάνεται ως έκτακτος υπάλληλος του Οργανισμού σύμφωνα με το άρθρο 2 στοιχείο α) του καθεστώτος που εφαρμόζεται στο λοιπό προσωπικό.
2. Ο εκτελεστικός διευθυντής διορίζεται από το διοικητικό συμβούλιο, από κατάλογο υποψηφίων που προτείνει η Επιτροπή, με ανοιχτή και διαφανή διαδικασία.
3. Για τη σύναψη της σύμβασης του εκτελεστικού διευθυντή, ο Οργανισμός εκπροσωπείται από τον πρόεδρο του διοικητικού συμβουλίου.
4. Πριν από τον διορισμό, ο υποψήφιος που έχει επιλεγεί από το διοικητικό συμβούλιο καλείται να προβεί σε δήλωση ενώπιον της σχετικής επιτροπής του Ευρωπαϊκού Κοινοβουλίου και να απαντήσει σε ερωτήσεις των βουλευτών.
5. Η θητεία του εκτελεστικού διευθυντή είναι πενταετής. Πριν από τη λήξη αυτής της περιόδου, η Επιτροπή διεξάγει αξιολόγηση στην οποία λαμβάνει υπόψη την αξιολόγηση των επιδόσεων του εκτελεστικού διευθυντή και τα μελλοντικά καθήκοντα και προκλήσεις του Οργανισμού.
6. Οι αποφάσεις του διοικητικού συμβουλίου σχετικά με τον διορισμό, την παράταση της θητείας ή την παύση του εκτελεστικού διευθυντή λαμβάνονται με πλειοψηφία των δύο τρίτων των μελών του με δικαίωμα ψήφου.
7. Το διοικητικό συμβούλιο μπορεί, με βάση πρόταση της Επιτροπής στην οποία λαμβάνεται υπόψη η αξιολόγηση που αναφέρεται στην παράγραφο 5, να παρατείνει άπαξ τη θητεία του εκτελεστικού διευθυντή, για διάστημα που δεν υπερβαίνει την πενταετία.
8. Το διοικητικό συμβούλιο γνωστοποιεί στο Ευρωπαϊκό Κοινοβούλιο την πρόθεσή του να παρατείνει τη θητεία του εκτελεστικού διευθυντή. Μέσα σε διάστημα τριών

μηνών πριν από την παράταση της θητείας του, ο εκτελεστικός διευθυντής, προβαίνει, αν λάβει σχετική πρόσκληση, σε δήλωση ενώπιον της σχετικής επιτροπής του Ευρωπαϊκού Κοινοβουλίου και απαντά σε ερωτήσεις των βουλευτών.

9. Εκτελεστικός διευθυντής του οποίου η θητεία έχει ανανεωθεί δεν επιτρέπεται να συμμετάσχει στη διαδικασία επιλογής για την ίδια θέση.

10. Ο εκτελεστικός διευθυντής μπορεί να απαλλαγεί από τα καθήκοντά του μόνο με απόφαση του διοικητικού συμβουλίου, κατόπιν πρότασης της Επιτροπής.

Άρθρο 34
Αποσπασμένοι εμπειρογνώμονες και λοιπό προσωπικό

1. Ο Οργανισμός μπορεί να χρησιμοποιεί αποσπασμένους εθνικούς εμπειρογνώμονες ή άλλο προσωπικό που δεν απασχολείται από τον Οργανισμό. Στο προσωπικό αυτό δεν εφαρμόζονται ο κανονισμός υπηρεσιακής κατάστασης και το καθεστώς που εφαρμόζεται στο λοιπό προσωπικό.

2. Το διοικητικό συμβούλιο λαμβάνει απόφαση με την οποία καθορίζει τους κανόνες για την απόσπαση εθνικών εμπειρογνωμόνων στον Οργανισμό.

ΚΕΦΑΛΑΙΟ V
ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 35
***Νομικό καθεστώς* του Οργανισμού**

1. Ο Οργανισμός αποτελεί όργανο της Ένωσης και διαθέτει νομική προσωπικότητα.

2. Σε κάθε κράτος μέλος, ο Οργανισμός διαθέτει την ευρύτερη δυνατή νομική ικανότητα που παρέχεται στα νομικά πρόσωπα βάσει του εθνικού δικαίου. Δύναται ιδίως να αποκτά και να διαθέτει κινητή και ακίνητη περιουσία και να παρίσταται ενώπιον δικαστηρίου ή αμφότερα.

3. Ο Οργανισμός εκπροσωπείται από τον εκτελεστικό διευθυντή του.

Άρθρο 36
Ευθύνη του Οργανισμού

1. Η συμβατική ευθύνη του Οργανισμού διέπεται από το εφαρμοστέο στην οικεία σύμβαση δίκαιο.

2. Το Δικαστήριο της Ευρωπαϊκής Ένωσης είναι αρμόδιο να αποφαίνεται δυνάμει ρήτρας διαιτησίας που περιλαμβάνεται σε σύμβαση που συνάπτει ο Οργανισμός.

3. Σε περίπτωση μη συμβατικής ευθύνης, ο Οργανισμός αποκαθιστά, σύμφωνα με τις γενικές αρχές που είναι κοινές στο δίκαιο των κρατών μελών, οποιαδήποτε ζημία προκαλείται από αυτόν ή από τους υπαλλήλους του κατά την εκτέλεση των καθηκόντων τους.

4. Το Δικαστήριο της Ευρωπαϊκής Ένωσης είναι αρμόδιο για την εκδίκαση οποιασδήποτε διαφοράς η οποία συνδέεται με την αποκατάσταση αυτών των ζημιών.

5. Η προσωπική ευθύνη των υπαλλήλων έναντι του Οργανισμού διέπεται από τους σχετικούς όρους που ισχύουν για το προσωπικό του Οργανισμού.

Άρθρο 37

Γλωσσικό καθεστώς

1. Ο Οργανισμός υπόκειται στις διατάξεις του κανονισμού αριθ. 1 του Συμβουλίου[41]. Τα κράτη μέλη και οι άλλοι φορείς τους οποίους ορίζουν μπορούν να απευθύνονται στον Οργανισμό και να λαμβάνουν απάντηση στην επίσημη γλώσσα των θεσμικών οργάνων της Ένωσης που επιλέγουν.

2. Οι μεταφραστικές υπηρεσίες που απαιτούνται για τη λειτουργία του Οργανισμού παρέχονται από το Μεταφραστικό Κέντρο των Οργάνων της Ευρωπαϊκής Ένωσης.

Άρθρο 38

Προστασία δεδομένων προσωπικού χαρακτήρα

1. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα από τον Οργανισμό υπόκειται στον κανονισμό (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[42].

2. Το διοικητικό συμβούλιο θεσπίζει τις διατάξεις εφαρμογής που αναφέρονται στο άρθρο 24 παράγραφος 8 του κανονισμού (ΕΚ) αριθ. 45/2001. Το διοικητικό συμβούλιο μπορεί να θεσπίζει τις πρόσθετες διατάξεις που απαιτούνται για την εφαρμογή του κανονισμού (ΕΚ) αριθ. 45/2001 από τον Οργανισμό.

Άρθρο 39

Συνεργασία με τρίτες χώρες και διεθνείς οργανισμούς

1. Στον βαθμό που είναι αναγκαίο για την επίτευξη των στόχων που καθορίζονται στον παρόντα κανονισμό, ο Οργανισμός δύναται να συνεργάζεται με τις αρμόδιες αρχές τρίτων χωρών ή με διεθνείς οργανισμούς ή και με τα δύο. Για τον σκοπό αυτό, ο Οργανισμός δύναται, κατόπιν προηγούμενης έγκρισης της Επιτροπής, να συνάπτει συμφωνίες συνεργασίας με τις εν λόγω αρχές τρίτων χωρών και διεθνείς οργανισμούς. Οι συμφωνίες αυτές δεν δημιουργούν έννομες υποχρεώσεις στην Ένωση και τα κράτη μέλη της.

2. Ο Οργανισμός είναι ανοικτός στη συμμετοχή τρίτων χωρών οι οποίες έχουν συνάψει σχετικές συμφωνίες με την Ευρωπαϊκή Ένωση. Σύμφωνα με τις σχετικές διατάξεις των εν λόγω συμφωνιών, θεσπίζονται ρυθμίσεις που ορίζουν, κυρίως, τη φύση, την έκταση και τον τρόπο συμμετοχής εκάστης των χωρών αυτών στο έργο του Οργανισμού, συμπεριλαμβανομένων διατάξεων σχετικών με τη συμμετοχή στις πρωτοβουλίες που αναλαμβάνει ο Οργανισμός, την οικονομική συμβολή και το προσωπικό. Στα ζητήματα προσωπικού, οι εν λόγω συμφωνίες τηρούν πάντοτε τον κανονισμό υπηρεσιακής κατάστασης.

3. Το διοικητικό συμβούλιο εγκρίνει στρατηγική σχέσεων με τρίτες χώρες ή διεθνείς οργανισμούς σχετικά με ζητήματα για τα οποία είναι αρμόδιος ο Οργανισμός. Η Επιτροπή διασφαλίζει ότι ο Οργανισμός λειτουργεί εντός των ορίων της εντολής του

---

41 Κανονισμός αριθ. 1 περί καθορισμού του γλωσσικού καθεστώτος της Ευρωπαϊκής Κοινότητας Ατομικής Ενέργειας (ΕΕ 17 της 6.10.1958, σ. 401).

42 Κανονισμός (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Δεκεμβρίου 2000, σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών (ΕΕ L 8 της 12.1.2001, σ. 1).

και του υπάρχοντος θεσμικού πλαισίου, μέσω της σύναψης κατάλληλης συμφωνίας συνεργασίας με τον εκτελεστικό διευθυντή του Οργανισμού.

Άρθρο 40

***Κανόνες* ασφάλειας για την προστασία διαβαθμισμένων και ευαίσθητων μη διαβαθμισμένων πληροφοριών**

Σε διαβούλευση με την Επιτροπή, ο Οργανισμός θεσπίζει τους κανόνες ασφάλειάς του εφαρμόζοντας τις αρχές ασφάλειας που περιέχονται στους κανόνες ασφάλειας της Επιτροπής σχετικά με την προστασία των διαβαθμισμένων πληροφοριών της Ευρωπαϊκής Ένωσης (ΔΠΕΕ) και των ευαίσθητων μη διαβαθμισμένων πληροφοριών, που καθορίζονται στην απόφαση (ΕΚ, Ευρατόμ) 2015/443 της Επιτροπής και στην απόφαση (ΕΚ, Ευρατόμ) 2015/444 της Επιτροπής. Τούτο καλύπτει, μεταξύ άλλων, τις διατάξεις που έχουν σχέση με την ανταλλαγή, την επεξεργασία και την αποθήκευση τέτοιων πληροφοριών.

Άρθρο 41

Συμφωνία σχετικά με την έδρα και όροι λειτουργίας

1. Οι απαραίτητες ρυθμίσεις για την εγκατάσταση του Οργανισμού στο κράτος μέλος υποδοχής και τα μέσα που πρέπει να τίθενται στη διάθεσή του από το εν λόγω κράτος μέλος, παράλληλα με τους ειδικούς κανόνες που εφαρμόζονται στο κράτος μέλος υποδοχής όσον αφορά τον εκτελεστικό διευθυντή, τα μέλη του διοικητικού συμβουλίου, το προσωπικό του Οργανισμού και τα μέλη των οικογενειών τους, ορίζονται σε συμφωνία για την έδρα του Οργανισμού η οποία συνάπτεται μεταξύ του Οργανισμού και του κράτους μέλους στο οποίο βρίσκεται η έδρα, μόλις ληφθεί η έγκριση του διοικητικού συμβουλίου και σε κάθε περίπτωση το αργότερο εντός [2 ετών από την έναρξη ισχύος του παρόντος κανονισμού].
2. Το κράτος μέλος υποδοχής του Οργανισμού εξασφαλίζει τις καλύτερες δυνατές συνθήκες για την εύρυθμη λειτουργία του Οργανισμού, συμπεριλαμβανομένων της προσβασιμότητας του τόπου εγκατάστασης, της ύπαρξης κατάλληλων εκπαιδευτικών δυνατοτήτων για τα τέκνα των υπαλλήλων, της κατάλληλης πρόσβασης στην αγορά εργασίας, της κοινωνικής ασφάλισης και της ιατροφαρμακευτικής φροντίδας τόσο για τα τέκνα όσο και για τις συζύγους.

Άρθρο 42

Διοικητικός έλεγχος

Οι δραστηριότητες του Οργανισμού υπόκεινται στην εποπτεία του Διαμεσολαβητή, σύμφωνα με τις διατάξεις του άρθρου 228 ΣΛΕΕ.

ΤΙΤΛΟΣ ΙΙΙ
ΠΛΑΙΣΙΟ ΠΙΣΤΟΠΟΙΗΣΗΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Άρθρο 43

Ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο

Ένα ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο βεβαιώνει ότι τα προϊόντα και οι υπηρεσίες ΤΠΕ που έχουν λάβει πιστοποίηση σύμφωνα με ένα τέτοιο σύστημα συμμορφώνονται με συγκεκριμένες απαιτήσεις όσον αφορά την ικανότητά τους να ανθίστανται, σε ένα δεδομένο επίπεδο διασφάλισης, σε ενέργειες οι οποίες θέτουν σε κίνδυνο τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα και την εμπιστευτικότητα αποθηκευμένων ή διαβιβαζόμενων ή επεξεργασμένων δεδομένων ή των σχετικών λειτουργιών ή των σχετικών υπηρεσιών που παρέχονται ή είναι προσβάσιμες μέσω των εν λόγω προϊόντων, διαδικασιών, υπηρεσιών και συστημάτων.

Άρθρο 44

Επεξεργασία και έγκριση ενός ευρωπαϊκού συστήματος πιστοποίησης της ασφάλειας στον κυβερνοχώρο

1. Κατόπιν αιτήματος της Επιτροπής, ο ENISA επεξεργάζεται ένα υποψήφιο ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο που πληροί τις απαιτήσεις που ορίζονται στα άρθρα 45, 46 και 47 του παρόντος κανονισμού. Τα κράτη μέλη ή η ευρωπαϊκή ομάδα πιστοποίησης της ασφάλειας στον κυβερνοχώρο (η «ομάδα»), που έχει συσταθεί βάσει του άρθρου 53, μπορεί να προτείνουν στην Επιτροπή την επεξεργασία ενός υποψήφιου ευρωπαϊκού συστήματος πιστοποίησης της ασφάλειας στον κυβερνοχώρο.

2. Κατά την επεξεργασία των υποψήφιων συστημάτων που αναφέρονται στην παράγραφο 1 του παρόντος άρθρου, ο ENISA συμβουλεύει όλους τους σχετικούς άμεσα ενδιαφερόμενους και συνεργάζεται στενά με την ομάδα. Η ομάδα παρέχει στον ENISA τη συνδρομή και την εμπειρογνωσία που αυτός ζητά σε σχέση με την επεξεργασία του υποψήφιου συστήματος, συμπεριλαμβανομένων γνωμοδοτήσεων, αν κρίνεται αναγκαίο.

3. Ο ENISA διαβιβάζει στην Επιτροπή το επεξεργασθέν υποψήφιο ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο, σύμφωνα με την παράγραφο 2 του παρόντος άρθρου.

4. Η Επιτροπή, με βάση το υποψήφιο σύστημα που προτείνει ο ENISA, μπορεί να εκδώσει εκτελεστικές πράξεις, δυνάμει του άρθρου 55 παράγραφος 1, οι οποίες προβλέπουν σε σχέση με ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο προϊόντα και υπηρεσίες ΤΠΕ που πληρούν τις απαιτήσεις των άρθρων 45, 46 και 47 του παρόντος κανονισμού.

5. Ο ENISA διατηρεί έναν ειδικό δικτυακό τόπο που παρέχει πληροφορίες και εξασφαλίζει την προβολή για τα ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο.

Άρθρο 45

Στόχοι ασφάλειας για τα ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο

Ένα ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο σχεδιάζεται κατά τέτοιο τρόπο ώστε να συνεκτιμά, κατά περίπτωση, τους ακόλουθους στόχους ασφάλειας:

α) την προστασία δεδομένων που έχουν αποθηκευτεί, διαβιβαστεί ή αποτελέσει με άλλο τρόπο αντικείμενο επεξεργασίας από τυχαία ή μη εγκεκριμένη αποθήκευση, επεξεργασία, πρόσβαση ή αποκάλυψη·

β) την προστασία δεδομένων που έχουν αποθηκευτεί, διαβιβαστεί ή αποτελέσει με άλλο τρόπο αντικείμενο επεξεργασίας από τυχαία ή μη εγκεκριμένη καταστροφή, τυχαία απώλεια ή αλλοίωση·

γ) τη διασφάλιση ότι εγκεκριμένα άτομα, προγράμματα ή μηχανήματα μπορούν να έχουν αποκλειστική πρόσβαση σε δεδομένα, υπηρεσίες ή λειτουργίες που καλύπτονται από το δικαίωμα πρόσβασης που τους παρέχεται·

δ) την καταγραφή των δεδομένων, λειτουργιών ή υπηρεσιών που έχουν κοινοποιηθεί, καθώς και πότε κοινοποιήθηκαν και από ποιον·

ε) τη διασφάλιση της δυνατότητας να ελέγχεται σε ποια δεδομένα, υπηρεσίες ή λειτουργίες πραγματοποιήθηκε πρόσβαση ή χρησιμοποιήθηκαν, πότε και από ποιον·

στ) την έγκαιρη αποκατάσταση της διαθεσιμότητας και της πρόσβασης σε δεδομένα, υπηρεσίες και λειτουργίες σε περίπτωση φυσικών ή τεχνικών συμβάντων·

ζ) τη διασφάλιση ότι τα προϊόντα και οι υπηρεσίες ΤΠΕ παρέχονται με επικαιροποιημένο λογισμικό που δεν περιέχει γνωστά τρωτά σημεία και ότι προβλέπονται μηχανισμοί για ασφαλείς επικαιροποιήσεις λογισμικού.

Άρθρο 46

Επίπεδα διασφάλισης των ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο

1. Ένα ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο μπορεί να προσδιορίζει ένα ή περισσότερα από τα ακόλουθα επίπεδα διασφάλισης: βασικό, σημαντικό και/ή υψηλό, για πιστοποιητικά προϊόντων και υπηρεσιών ΤΠΕ που εκδίδονται στο πλαίσιο του εν λόγω συστήματος.

2. Το βασικό, το σημαντικό και το υψηλό επίπεδο διασφάλισης πληρούν αντιστοίχως τα ακόλουθα κριτήρια:

α) το βασικό επίπεδο διασφάλισης αναφέρεται σε πιστοποιητικό εκδιδόμενο στο πλαίσιο ενός ευρωπαϊκού συστήματος πιστοποίησης της ασφάλειας στον κυβερνοχώρο, το οποίο παρέχει περιορισμένο βαθμό εμπιστοσύνης στις ιδιότητες ασφάλειας στον κυβερνοχώρο που επικαλείται ή δηλώνει ένα προϊόν ή μια υπηρεσία ΤΠΕ, και στο οποίο αποδίδεται χαρακτηρισμός βάσει των σχετικών τεχνικών προδιαγραφών, προτύπων και διαδικασιών, συμπεριλαμβανομένων των τεχνικών ελέγχων, σκοπός των οποίων είναι η

μείωση του κινδύνου συμβάντων που αφορούν την ασφάλεια στον κυβερνοχώρο·

β) το σημαντικό επίπεδο διασφάλισης αναφέρεται σε πιστοποιητικό εκδιδόμενο στο πλαίσιο ενός ευρωπαϊκού συστήματος πιστοποίησης της ασφάλειας στον κυβερνοχώρο, το οποίο παρέχει σημαντικό βαθμό εμπιστοσύνης στις ιδιότητες ασφάλειας στον κυβερνοχώρο που επικαλείται ή δηλώνει ένα προϊόν ή μια υπηρεσία ΤΠΕ, και στο οποίο αποδίδεται χαρακτηρισμός βάσει των σχετικών τεχνικών προδιαγραφών, προτύπων και διαδικασιών, περιλαμβανομένων των τεχνικών ελέγχων, σκοπός των οποίων είναι η σημαντική μείωση του κινδύνου συμβάντων που αφορούν την ασφάλεια στον κυβερνοχώρο·

γ) το υψηλό επίπεδο διασφάλισης αναφέρεται σε πιστοποιητικό εκδιδόμενο στο πλαίσιο ενός ευρωπαϊκού συστήματος πιστοποίησης της ασφάλειας στον κυβερνοχώρο, το οποίο παρέχει υψηλό βαθμό εμπιστοσύνης στις ιδιότητες ασφάλειας στον κυβερνοχώρο που επικαλείται ή δηλώνει ένα προϊόν ή μια υπηρεσία ΤΠΕ, και στο οποίο αποδίδεται χαρακτηρισμός βάσει των σχετικών τεχνικών προδιαγραφών, προτύπων και διαδικασιών, περιλαμβανομένων των τεχνικών ελέγχων, σκοπός των οποίων είναι η αποτροπή συμβάντων που αφορούν την ασφάλεια στον κυβερνοχώρο.

Άρθρο 47

Στοιχεία των ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο

1. Ένα ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο περιλαμβάνει τα ακόλουθα στοιχεία:

α) το αντικείμενο και το πεδίο εφαρμογής της πιστοποίησης, συμπεριλαμβανομένων του τύπου ή των κατηγοριών των καλυπτόμενων προϊόντων και υπηρεσιών ΤΠΕ·

β) τον λεπτομερή καθορισμό των σχετικών με την ασφάλεια στον κυβερνοχώρο απαιτήσεων με γνώμονα τις οποίες αξιολογούνται τα συγκεκριμένα προϊόντα ή οι συγκεκριμένες υπηρεσίες ΤΠΕ, για παράδειγμα με αναφορά σε ενωσιακά ή διεθνή πρότυπα ή σε τεχνικές προδιαγραφές·

γ) όπου συντρέχει περίπτωση, ένα ή περισσότερα επίπεδα διασφάλισης·

δ) τα ειδικά κριτήρια και τις μεθόδους αξιολόγησης που χρησιμοποιούνται, συμπεριλαμβανομένων των τύπων αξιολόγησης, προκειμένου να καταδεικνύεται ότι επιτυγχάνονται οι συγκεκριμένοι στόχοι που αναφέρονται στο άρθρο 45·

ε) τις πληροφορίες που παρέχονται στους οργανισμούς αξιολόγησης της συμμόρφωσης από κάποιον αιτούντα και είναι απαραίτητες για την πιστοποίηση·

στ) σε περίπτωση που το σύστημα προβλέπει σήματα ή επισημάνσεις, τις προϋποθέσεις υπό τις οποίες είναι δυνατή η χρήση τέτοιων σημάτων ή επισημάνσεων·

ζ) σε περίπτωση που το σύστημα περιλαμβάνει εποπτεία, τους κανόνες παρακολούθησης της συμμόρφωσης με τις απαιτήσεις των πιστοποιητικών, συμπεριλαμβανομένων των μηχανισμών για την κατάδειξη της συνεχούς συμμόρφωσης με τις συγκεκριμένες απαιτήσεις της ασφάλειας στον κυβερνοχώρο·

η) τις προϋποθέσεις για τη χορήγηση, τη διατήρηση, τη συνέχιση, την επέκταση και τον περιορισμό του πεδίου εφαρμογής της πιστοποίησης·

θ) τους κανόνες σχετικά με τις συνέπειες της μη συμμόρφωσης των πιστοποιημένων προϊόντων και υπηρεσιών ΤΠΕ με τις απαιτήσεις πιστοποίησης·

ι) τους κανόνες σχετικά με τον τρόπο που τα προηγουμένως μη διαπιστωθέντα σχετικά με την ασφάλεια στον κυβερνοχώρο τρωτά σημεία προϊόντων και υπηρεσιών ΤΠΕ πρέπει να αναφέρονται και να αντιμετωπίζονται·

ια) τους κανόνες σχετικά με την τήρηση μητρώων από τους οργανισμούς αξιολόγησης της συμμόρφωσης·

ιβ) τον προσδιορισμό εθνικών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο που καλύπτουν τον ίδιο τύπο ή τις ίδιες κατηγορίες προϊόντων και υπηρεσιών ΤΠΕ·

ιγ) το περιεχόμενο του εκδιδόμενου πιστοποιητικού.

2. Οι καθορισμένες απαιτήσεις του συστήματος δεν πρέπει να αντιβαίνουν τυχόν εφαρμοστέες νομικές απαιτήσεις, ιδίως όσον αφορά απαιτήσεις προερχόμενες από την εναρμονισμένη ενωσιακή νομοθεσία.

3. Σε περίπτωση που κάτι τέτοιο προβλέπεται από συγκεκριμένη πράξη της Ένωσης, η πιστοποίηση στο πλαίσιο ενός ευρωπαϊκού συστήματος πιστοποίησης της ασφάλειας στον κυβερνοχώρο μπορεί να χρησιμοποιείται για να καταδεικνύει το τεκμήριο συμμόρφωσης με τις απαιτήσεις της εν λόγω πράξης.

4. Εφόσον δεν υπάρχει εναρμονισμένη ενωσιακή νομοθεσία, η νομοθεσία των κρατών μελών μπορεί επίσης να προβλέπει ότι ένα ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο μπορεί να χρησιμοποιείται για τη θέσπιση του τεκμήριου συμμόρφωσης με τις νομικές απαιτήσεις.

Άρθρο 48

Πιστοποίηση της ασφάλειας στον κυβερνοχώρο

1. Τα προϊόντα και οι υπηρεσίες ΤΠΕ που έχουν πιστοποιηθεί στο πλαίσιο ενός ευρωπαϊκού συστήματος πιστοποίησης της ασφάλειας στον κυβερνοχώρο που εγκρίνεται δυνάμει του άρθρου 44 τεκμαίρονται ότι πληρούν τις απαιτήσεις ενός τέτοιου συστήματος.

2. Η πιστοποίηση είναι εθελοντική, εκτός αν άλλως ορίζεται στη νομοθεσία της Ένωσης.

3. Ένα ευρωπαϊκό πιστοποιητικό ασφάλειας στον κυβερνοχώρο δυνάμει του παρόντος άρθρου εκδίδεται από τους οργανισμούς αξιολόγησης της συμμόρφωσης που

αναφέρονται στο άρθρο 51 βάσει κριτηρίων που περιλαμβάνονται στο ευρωπαϊκό σύστημα ασφάλειας στον κυβερνοχώρο, εγκριθέντος δυνάμει του άρθρου 44.

4. Κατά παρέκκλιση από την παράγραφο 3, σε δεόντως αιτιολογημένες περιπτώσεις, ένα συγκεκριμένο ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο μπορεί να προβλέπει ότι ένα ευρωπαϊκό πιστοποιητικό ασφάλειας στον κυβερνοχώρο που προκύπτει από το εν λόγω σύστημα μπορεί να εκδίδεται μόνο από δημόσιο οργανισμό. Ένας τέτοιος δημόσιος οργανισμός μπορεί να είναι:

α) μια εθνική εποπτική αρχή πιστοποίησης όπως αναφέρεται στο άρθρο 50 παράγραφος 1·

β) ένας οργανισμός που λαμβάνει διαπίστευση ως οργανισμός αξιολόγησης της συμμόρφωσης δυνάμει του άρθρου 51 παράγραφος 1 ή

γ) ένας οργανισμός που θεσπίζεται βάσει νόμων, κανονιστικών πράξεων ή άλλων επίσημων διοικητικών διαδικασιών οικείου κράτους μέλους και πληροί τις απαιτήσεις για τους οργανισμούς που πιστοποιούν προϊόντα, διαδικασίες και υπηρεσίες στο πλαίσιο του ISO/IEC 17065:2012.

5. Το φυσικό ή νομικό πρόσωπο που υποβάλλει τα προϊόντα ή τις υπηρεσίες ΤΠΕ του στον μηχανισμό πιστοποίησης παρέχει στον οργανισμό αξιολόγησης της συμμόρφωσης που αναφέρεται στο άρθρο 51 όλες τις πληροφορίες που απαιτούνται για τη διενέργεια της διαδικασίας πιστοποίησης.

6. Τα πιστοποιητικά εκδίδονται για μέγιστη περίοδο τριών ετών και μπορούν να ανανεώνονται, υπό τις ίδιες συνθήκες, με την προϋπόθεση ότι εξακολουθούν να πληρούνται οι σχετικές απαιτήσεις.

7. Ένα ευρωπαϊκό πιστοποιητικό ασφάλειας στον κυβερνοχώρο που εκδίδεται δυνάμει του παρόντος άρθρου αναγνωρίζεται σε όλα τα κράτη μέλη.

Άρθρο 49

Εθνικά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο και σχετικά πιστοποιητικά

1. Με την επιφύλαξη της παραγράφου 3, τα εθνικά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο και οι σχετικές διαδικασίες για τα προϊόντα και τις υπηρεσίες ΤΠΕ που καλύπτονται από ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο παύουν να παράγουν αποτελέσματα από την ημερομηνία που ορίζεται στην εκτελεστική πράξη που εκδίδεται σύμφωνα με το άρθρο 44 παράγραφος 4. Τα υφιστάμενα εθνικά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο και οι σχετικές διαδικασίες για τα προϊόντα και τις υπηρεσίες ΤΠΕ που δεν καλύπτονται από ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο συνεχίζουν να παράγουν αποτελέσματα.

2. Τα κράτη μέλη δεν θεσπίζουν νέα εθνικά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο για τα προϊόντα και τις υπηρεσίες ΤΠΕ που καλύπτονται από ισχύον ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο.

3. Τα υφιστάμενα πιστοποιητικά που έχουν εκδοθεί στο πλαίσιο εθνικών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο παραμένουν σε ισχύ έως την ημερομηνία λήξης τους.

Άρθρο 50

Εθνικές εποπτικές αρχές πιστοποίησης

1. Κάθε κράτος μέλος ορίζει μια εθνική εποπτική αρχή πιστοποίησης.

2. Κάθε κράτος μέλος ενημερώνει την Επιτροπή για την ταυτότητα της οριζόμενης αρχής.

3. Οι εθνικές εποπτικές αρχές πιστοποίησης είναι ανεξάρτητες, σε επίπεδο οργάνωσης, αποφάσεων χρηματοδότησης, νομικής διάρθρωσης και λήψης αποφάσεων, από τις οντότητες τις οποίες επιβλέπουν.

4. Τα κράτη μέλη μεριμνούν ώστε οι εθνικές εποπτικές αρχές πιστοποίησης να έχουν στη διάθεσή τους επαρκείς πόρους για την άσκηση των αρμοδιοτήτων τους και να ασκούν, με αποδοτικό και αποτελεσματικό τρόπο, τα καθήκοντα που τους έχουν ανατεθεί.

5. Για την αποτελεσματική εφαρμογή του κανονισμού, οι εν λόγω αρχές είναι σκόπιμο να συμμετέχουν στην ευρωπαϊκή ομάδα πιστοποίησης της ασφάλειας στον κυβερνοχώρο που συστήνεται δυνάμει του άρθρου 53 με ενεργό, αποτελεσματικό, αποδοτικό και ασφαλή τρόπο.

6. Οι εθνικές εποπτικές αρχές πιστοποίησης:

   α) παρακολουθούν και μεριμνούν για την εφαρμογή των διατάξεων του παρόντος τίτλου σε εθνικό επίπεδο και εποπτεύουν τη συμμόρφωση των πιστοποιητικών που έχουν εκδοθεί από τους αρμόδιους οργανισμούς αξιολόγησης της συμμόρφωσης στις επικράτειές τους με τις απαιτήσεις που θεσπίζονται στον παρόντα τίτλο και στο αντίστοιχο ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο·

   β) παρακολουθούν και εποπτεύουν τις δραστηριότητες των οργανισμών αξιολόγησης της συμμόρφωσης στο πλαίσιο του παρόντος κανονισμού, μεταξύ άλλων όσον αφορά την κοινοποίηση των οργανισμών αξιολόγησης της συμμόρφωσης και τις σχετικές ενέργειες όπως ορίζονται στο άρθρο 52 του παρόντος κανονισμού·

   γ) διεκπεραιώνουν καταγγελίες τις οποίες υποβάλλουν φυσικά ή νομικά πρόσωπα σε σχέση με πιστοποιητικά που έχουν εκδοθεί από τους αρμόδιους οργανισμούς αξιολόγησης της συμμόρφωσης στις επικράτειές τους, διερευνούν, στον βαθμό που ενδείκνυται, το αντικείμενο της καταγγελίας, και ενημερώνουν τον καταγγέλλοντα σχετικά με την πρόοδο και το αποτέλεσμα της έρευνας εντός εύλογου χρονικού διαστήματος·

   δ) συνεργάζονται με άλλες εθνικές εποπτικές αρχές πιστοποίησης ή άλλες δημόσιες αρχές, μεταξύ άλλων μέσω της ανταλλαγής πληροφοριών σχετικά με πιθανή μη συμμόρφωση προϊόντων και υπηρεσιών ΤΠΕ με τις απαιτήσεις του παρόντος κανονισμού ή συγκεκριμένα ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο·

   ε) παρακολουθούν τις σχετικές εξελίξεις στον τομέα της πιστοποίησης της ασφάλειας στον κυβερνοχώρο.

7. Οι εθνικές εποπτικές αρχές πιστοποίησης έχουν κατ' ελάχιστον τις ακόλουθες εξουσίες:

α) να ζητούν από τους οργανισμούς αξιολόγησης της συμμόρφωσης και τους κατόχους ευρωπαϊκού πιστοποιητικού ασφάλειας στον κυβερνοχώρο να προσκομίσουν τις πληροφορίες που απαιτούνται για την άσκηση των καθηκόντων τους·

β) να διενεργούν έρευνες, υπό μορφή ελέγχων, των οργανισμών αξιολόγησης της συμμόρφωσης και των κατόχων ευρωπαϊκού πιστοποιητικού ασφάλειας στον κυβερνοχώρο, με στόχο τον έλεγχο της συμμόρφωσης με τις διατάξεις του τίτλου ΙΙΙ·

γ) να λαμβάνουν τα ενδεδειγμένα μέτρα, σύμφωνα με την εθνική νομοθεσία, προκειμένου να διασφαλίζεται η συμμόρφωση των οργανισμών αξιολόγησης της συμμόρφωσης και των κατόχων πιστοποιητικού με τον παρόντα κανονισμό ή με ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο·

δ) να έχουν πρόσβαση στους χώρους των οργανισμών αξιολόγησης της συμμόρφωσης και των κατόχων ευρωπαϊκού πιστοποιητικού της ασφάλειας στον κυβερνοχώρο με σκοπό τη διενέργεια ερευνών σύμφωνα με το δικονομικό δίκαιο της Ένωσης ή των κρατών μελών·

ε) να ανακαλούν, σύμφωνα με την εθνική νομοθεσία, πιστοποιητικά που δεν συμμορφώνονται με τον παρόντα κανονισμό ή με ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο·

στ) να επιβάλλουν κυρώσεις, όπως προβλέπεται στο άρθρο 54, σε συμφωνία με το εθνικό δίκαιο, και να απαιτούν άμεση παύση των παραβιάσεων υποχρεώσεων οι οποίες θεσπίζονται στον παρόντα κανονισμό.

8. Οι εθνικές εποπτικές αρχές πιστοποίησης συνεργάζονται μεταξύ τους και με την Επιτροπή και, πιο συγκεκριμένα, ανταλλάσσουν πληροφορίες, εμπειρίες και ορθές πρακτικές όσον αφορά την πιστοποίηση της ασφάλειας στον κυβερνοχώρο και τα τεχνικά ζητήματα που αφορούν την ασφάλεια στον κυβερνοχώρο των προϊόντων και υπηρεσιών ΤΠΕ.

Άρθρο 51
Οργανισμοί αξιολόγησης της συμμόρφωσης

1. Οι οργανισμοί αξιολόγησης της συμμόρφωσης λαμβάνουν διαπίστευση από τον εθνικό οργανισμό διαπίστευσης που έχει οριστεί σύμφωνα με τον κανονισμό (ΕΚ) αριθ. 765/2008 μόνον εφόσον πληρούν τις απαιτήσεις που θεσπίζονται στο παράρτημα του παρόντος κανονισμού.

2. Η διαπίστευση χορηγείται για μέγιστη περίοδο πέντε ετών και μπορεί να ανανεωθεί με τους ίδιους όρους, υπό την προϋπόθεση ότι ο οργανισμός αξιολόγησης της συμμόρφωσης πληροί τις απαιτήσεις του παρόντος άρθρου. Οι οργανισμοί διαπίστευσης ανακαλούν τη διαπίστευση οργανισμού αξιολόγησης της συμμόρφωσης βάσει της παραγράφου 1 του παρόντος άρθρου όταν δεν πληρούνται, ή δεν πληρούνται πλέον, οι όροι για τη διαπίστευση ή όταν οι ενέργειες ενός οργανισμού αξιολόγησης της συμμόρφωσης παραβιάζουν τον παρόντα κανονισμό.

Άρθρο 52
Κοινοποίηση

1. Για κάθε ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο που εγκρίνεται σύμφωνα με το άρθρο 44, οι εθνικές εποπτικές αρχές πιστοποίησης κοινοποιούν στην Επιτροπή τους διαπιστευμένους οργανισμούς αξιολόγησης της συμμόρφωσης που είναι διαπιστευμένοι να εκδίδουν πιστοποιητικά σε συγκεκριμένα επίπεδα διασφάλισης όπως προβλέπεται στο άρθρο 46 και κάθε μεταγενέστερη σχετική μεταβολή, χωρίς αδικαιολόγητη καθυστέρηση.

2. Με τη συμπλήρωση έτους από την έναρξη εφαρμογής ενός ευρωπαϊκού συστήματος πιστοποίησης της ασφάλειας στον κυβερνοχώρο, η Επιτροπή δημοσιεύει κατάλογο των κοινοποιηθέντων οργανισμών αξιολόγησης της συμμόρφωσης στην Επίσημη Εφημερίδα.

3. Εάν η Επιτροπή λάβει κοινοποίηση μετά την πάροδο της αναφερόμενης στην παράγραφο 2 περιόδου, δημοσιεύει στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης τις τροποποιήσεις του καταλόγου της παραγράφου 2 εντός δύο μηνών από την ημερομηνία παραλαβής της εν λόγω κοινοποίησης.

4. Μια εθνική εποπτική αρχή πιστοποίησης μπορεί να υποβάλει στην Επιτροπή αίτημα διαγραφής οργανισμού αξιολόγησης της συμμόρφωσης, που κοινοποιήθηκε από τη συγκεκριμένη εθνική εποπτική αρχή πιστοποίησης, από τον κατάλογο που αναφέρεται στην παράγραφο 2 του παρόντος άρθρου. Η Επιτροπή δημοσιεύει στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης τις αντίστοιχες τροποποιήσεις του καταλόγου εντός μηνός από την ημερομηνία παραλαβής του αιτήματος που υποβάλλεται από την εθνική εποπτική αρχή πιστοποίησης.

5. Η Επιτροπή δύναται να καθορίζει, με την έκδοση εκτελεστικών πράξεων, τις συνθήκες, τη μορφή και τις διαδικασίες που ισχύουν για τις κοινοποιήσεις που αναφέρονται στην παράγραφο 1 του παρόντος άρθρου. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 55 παράγραφος 2.

Άρθρο 53
Ευρωπαϊκή ομάδα πιστοποίησης της ασφάλειας στον κυβερνοχώρο

1. Συστήνεται ευρωπαϊκή ομάδα πιστοποίησης της ασφάλειας στον κυβερνοχώρο (εφεξής η «ομάδα»).

2. Η ομάδα απαρτίζεται από τις εθνικές εποπτικές αρχές πιστοποίησης της ασφάλειας στον κυβερνοχώρο. Οι αρχές εκπροσωπούνται από τους επικεφαλής ή από άλλους εκπροσώπους υψηλού επιπέδου των εθνικών αρχών πιστοποίησης της ασφάλειας στον κυβερνοχώρο.

3. Η ομάδα έχει ως αποστολή:

   α) να συμβουλεύει και να συνδράμει την Επιτροπή στην προσπάθειά της να διασφαλίσει τη συνεπή υλοποίηση και εφαρμογή του παρόντος τίτλου, ιδίως όσον αφορά τα ζητήματα της πολιτικής πιστοποίησης της ασφάλειας στον κυβερνοχώρο, τον συντονισμό των προσεγγίσεων πολιτικής, και την επεξεργασία ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο·

β) να συνδράμει, να συμβουλεύει και να συνεργάζεται με τον ENISA κατά την επεξεργασία ενός υποψήφιου συστήματος σύμφωνα με το άρθρο 44 του παρόντος κανονισμού·

γ) να εισηγείται στην Επιτροπή την υποβολή αιτήματος στον Οργανισμό προκειμένου να προχωρήσει στην επεξεργασία υποψήφιου ευρωπαϊκού συστήματος πιστοποίησης ασφάλειας στον κυβερνοχώρο σύμφωνα με το άρθρο 44 του παρόντος κανονισμού·

δ) να εκδίδει γνώμες που απευθύνονται στην Επιτροπή σχετικά με τη διατήρηση και επανεξέταση των υφιστάμενων ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο·

ε) να εξετάζει τις σχετικές εξελίξεις στον τομέα της πιστοποίησης της ασφάλειας στον κυβερνοχώρο και της ανταλλαγής ορθών πρακτικών σε σχέση με τα συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο·

στ) να διευκολύνει τη συνεργασία μεταξύ των εθνικών εποπτικών αρχών πιστοποίησης βάσει του παρόντος τίτλου μέσω της ανταλλαγής πληροφοριών, καθιερώνοντας, ειδικότερα, μεθόδους για την αποτελεσματική ανταλλαγή πληροφοριών σχετικά με όλα τα θέματα που αφορούν την πιστοποίηση της ασφάλειας στον κυβερνοχώρο.

4. Η Επιτροπή προεδρεύει της ομάδας και της παρέχει γραμματειακή υποστήριξη, με την συνδρομή του ENISA όπως ορίζεται στο άρθρο 8 στοιχείο α).

Άρθρο 54
Κυρώσεις

Τα κράτη μέλη καθορίζουν τους κανόνες για τις κυρώσεις οι οποίες επιβάλλονται σε περίπτωση παραβίασης των διατάξεων του παρόντος τίτλου και των ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο και λαμβάνουν όλα τα αναγκαία μέτρα προκειμένου να εξασφαλίσουν την επιβολή τους. Οι προβλεπόμενες κυρώσεις είναι αποτελεσματικές, αναλογικές και αποτρεπτικές. Τα κράτη μέλη κοινοποιούν στην Επιτροπή [έως …/χωρίς καθυστέρηση] τους εν λόγω κανόνες και μέτρα και την ενημερώνουν σχετικά με κάθε μεταγενέστερη τροποποίηση τους που τους επηρεάζει.

ΤΙΤΛΟΣ IV
ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 55
Διαδικασία επιτροπής

1. Η Επιτροπή επικουρείται από επιτροπή. Η εν λόγω επιτροπή αποτελεί επιτροπή κατά την έννοια του κανονισμού (ΕΕ) αριθ. 182/2011.

2. Όταν γίνεται αναφορά στην παρούσα παράγραφο, εφαρμόζεται το άρθρο 4 του κανονισμού (ΕΕ) αριθ. 182/2011.

Άρθρο 56
Αξιολόγηση και επανεξέταση

1. Το αργότερο πέντε έτη μετά την ημερομηνία που αναφέρεται στο άρθρο 58 και στη συνέχεια ανά πενταετία, η Επιτροπή αξιολογεί τον αντίκτυπο, την αποτελεσματικότητα και την απόδοση του Οργανισμού και των εργασιακών πρακτικών του, καθώς και τη δυνατότητα για ενδεχόμενη τροποποίηση της εντολής του Οργανισμού, και τις δημοσιονομικές επιπτώσεις οποιασδήποτε τέτοιας τροποποίησης. Στην αξιολόγηση λαμβάνονται υπόψη οι αντιδράσεις που έχουν τεθεί υπόψη του Οργανισμού σε σχέση με τις δραστηριότητές του. Σε περίπτωση που η Επιτροπή κρίνει ότι η συνέχιση της ύπαρξης του Οργανισμού δεν δικαιολογείται πλέον σε σχέση με τους προκαθορισμένους στόχους, την εντολή και τα καθήκοντά του, μπορεί να εισηγηθεί την τροποποίηση του παρόντος κανονισμού ως προς τις διατάξεις που αφορούν τον Οργανισμό.

2. Η αξιολόγηση εξετάζει επίσης τον αντίκτυπο, την αποτελεσματικότητα και την απόδοση των διατάξεων του τίτλου ΙΙΙ σε σχέση με τους στόχους αφενός της διασφάλισης επαρκούς επιπέδου ασφάλειας στον κυβερνοχώρο των προϊόντων και υπηρεσιών ΤΠΕ στην Ένωση και αφετέρου της βελτίωσης της λειτουργίας της εσωτερικής αγοράς.

3. Η Επιτροπή διαβιβάζει την έκθεση αξιολόγησης μαζί με τα συμπεράσματά της στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και το διοικητικό συμβούλιο. Τα συμπεράσματα της έκθεσης αξιολόγησης δημοσιοποιούνται.

Άρθρο 57
Κατάργηση και διαδοχή

1. Ο κανονισμός (ΕΚ) αριθ. 526/2013 καταργείται από την [….].

2. Οι παραπομπές στον κανονισμό (ΕΚ) αριθ. 526/2013 και στον ENISA θεωρείται ότι αποτελούν παραπομπές στον παρόντα κανονισμό και στον Οργανισμό.

3. Ο Οργανισμός διαδέχεται τον οργανισμό που συστάθηκε δυνάμει του κανονισμού (ΕΚ) αριθ. 526/2013 όσον αφορά όλα τα δικαιώματα ιδιοκτησίας, τις συμφωνίες, τις νομικές υποχρεώσεις, τις συμβάσεις εργασίας, τις οικονομικές δεσμεύσεις και ευθύνες. Όλες οι υφιστάμενες αποφάσεις του διοικητικού συμβουλίου και του εκτελεστικού συμβουλίου παραμένουν σε ισχύ, εφόσον δεν έρχονται σε σύγκρουση με τις διατάξεις του παρόντος κανονισμού.

4. Ο Οργανισμός ιδρύεται για απεριόριστο χρονικό διάστημα από την […].

5. Ο εκτελεστικός διευθυντής που διορίζεται βάσει του άρθρου 24 παράγραφος 4 του κανονισμού (ΕΚ) αριθ. 526/2013 αναλαμβάνει εκτελεστικός διευθυντής του Οργανισμού για το υπόλοιπο της θητείας του.

6. Τα τακτικά και τα αναπληρωματικά μέλη του διοικητικού συμβουλίου που διορίζονται βάσει του άρθρου 6 του κανονισμού (ΕΚ) αριθ. 526/2013 αναλαμβάνουν τακτικά και αναπληρωματικά μέλη του διοικητικού συμβουλίου του Οργανισμού για το υπόλοιπο της θητείας τους.

Άρθρο 58

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

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

Βρυξέλλες,

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

ΝΟΜΟΘΕΤΙΚΟ ΔΗΜΟΣΙΟΝΟΜΙΚΟ ΔΕΛΤΙΟ

1. ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

1.1. Τίτλος της πρότασης/πρωτοβουλίας

Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τον ENISA, τον «οργανισμό της ΕΕ για την ασφάλεια στον κυβερνοχώρο», και την κατάργηση του κανονισμού (ΕΕ) 526/2013, καθώς και σχετικά με την πιστοποίηση της ασφάλειας στον κυβερνοχώρο στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών («πράξη/κανονισμός για την ασφάλεια στον κυβερνοχώρο»)

1.2. Σχετικός/-οι τομέας/-είς πολιτικής

Τομέας πολιτικής: 09 - Επικοινωνιακά δίκτυα, περιεχόμενο και τεχνολογίες

Δραστηριότητα: 09.02 ψηφιακή ενιαία αγορά

1.3. Χαρακτήρας της πρότασης/πρωτοβουλίας

☒ Η πρόταση/πρωτοβουλία αφορά **νέα δράση (Τίτλος ΙΙΙ– Πιστοποίηση)**

☐ Η πρόταση/πρωτοβουλία αφορά **νέα δράση μετά από πιλοτικό έργο/προπαρασκευαστική δράση**[43]

☒Η πρόταση/πρωτοβουλία αφορά την **παράταση υφιστάμενης δράσης** (**Τίτλος ΙΙ – Θητεία του ENISA)**

☐ Η πρόταση/πρωτοβουλία αφορά **δράση προσανατολισμένη σε νέα δράση**

1.4. Στόχος(-οι)

1.4.1. Ο (Οι) πολυετής(-είς) στρατηγικός(-οί) στόχος(-οι) της Επιτροπής τον(τους) οποίο(-ους) αφορά η πρόταση/πρωτοβουλία

1. Ενίσχυση της ανθεκτικότητας των κρατών μελών, των επιχειρήσεων και της ΕΕ συνολικά

2. Διασφάλιση της εύρυθμης λειτουργίας της εσωτερικής αγοράς της ΕΕ για τα προϊόντα και τις υπηρεσίες ΤΠΕ

3. Αύξηση της ανταγωνιστικότητας, σε παγκόσμιο επίπεδο, των εταιρειών της ΕΕ που δραστηριοποιούνται στον κλάδο ΤΠΕ.

4. Προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που απαιτούν ασφάλεια στον κυβερνοχώρο.

1.4.2. Ειδικός(-οί) στόχος(-οι)

Με πυξίδα τους γενικούς στόχους, στο ευρύτερο πλαίσιο της αναθεωρημένης Στρατηγικής για την ασφάλεια στον κυβερνοχώρο, το μέσο, οριοθετώντας το πεδίο δράσης και την εντολή του ENISA και θεσπίζοντας ευρωπαϊκό πλαίσιο πιστοποίησης για τα προϊόντα και τις υπηρεσίες ΤΠΕ, επιδιώκει την επίτευξη των ακόλουθων ειδικών στόχων:

1. Αύξηση των **ικανοτήτων και της ετοιμότητας** των κρατών μελών και των επιχειρήσεων.
2. Βελτίωση της **συνεργασίας και του συντονισμού** στα κράτη μέλη και τα θεσμικά

[43] Όπως αναφέρονται στο άρθρο 54 παράγραφος 2 στοιχείο α) ή β) του δημοσιονομικού κανονισμού.

και λοιπά όργανα και τους οργανισμούς της ΕΕ.

3. Αύξηση των **ικανοτήτων σε επίπεδο ΕΕ για τη συμπλήρωση της δράσης των κρατών μελών**, ιδίως στην περίπτωση των διασυνοριακών κρίσεων στον κυβερνοχώρο.
4. Αύξηση της **ευαισθητοποίησης** των πολιτών και των επιχειρήσεων σε ζητήματα ασφάλειας στον κυβερνοχώρο.
5. Ενίσχυση της εμπιστοσύνης στην ψηφιακή ενιαία αγορά και στην ψηφιακή καινοτομία μέσα από την αύξηση της συνολικής **διαφάνειας της διασφάλισης της ασφάλειας στον κυβερνοχώρο**[44] των προϊόντων και υπηρεσιών ΤΠΕ.

Ο ENISA θα συμβάλει στην επίτευξη των ανωτέρω στόχων μέσα από:

Ενίσχυση της στήριξης στη χάραξη πολιτικής – παροχή καθοδήγησης και συμβουλών στην Επιτροπή και στα κράτη μέλη για την επικαιροποίηση και ανάπτυξη ενός ολοκληρωμένου κανονιστικού πλαισίου στον τομέα της ασφάλειας στον κυβερνοχώρο καθώς και ειδικών ανά τομέα πρωτοβουλιών σε επίπεδο πολιτικής και νομοθεσίας για τα ζητήματα ασφάλειας στον κυβερνοχώρο· συμβολή στις εργασίες της ομάδας συνεργασίας (άρθρο 11 της οδηγίας (ΕΕ) 2016/1148) με παροχή εμπειρογνωσίας και συνδρομής)· υποστήριξη της ανάπτυξης και υλοποίησης πολιτικών στον τομέα των υπηρεσιών ηλεκτρονικής ταυτοποίησης και εμπιστοσύνης· προαγωγή της ανταλλαγής βέλτιστων πρακτικών μεταξύ των αρμόδιων αρχών.

Ενίσχυση της στήριξης στην ανάπτυξη ικανοτήτων - παροχή υποστήριξης στα κράτη μέλη και στα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης με στόχο την ανάπτυξη και βελτίωση της πρόληψης, του εντοπισμού της ανάλυσης καθώς και της ικανότητας αντιμετώπισης προβλημάτων και συμβάντων σχετικών με την ασφάλεια στον κυβερνοχώρο· συνδρομή των κρατών μελών, μετά από αίτημά τους, στην ανάπτυξη εθνικών CSIRT, εθνικών στρατηγικών για την ασφάλεια στον κυβερνοχώρο· συνδρομή των οργάνων της Ένωσης στην ανάπτυξη και επανεξέταση των ενωσιακών στρατηγικών για την ασφάλεια στον κυβερνοχώρο· παροχή εκπαίδευσης στον τομέα της ασφάλειας στον κυβερνοχώρο· συνδρομή των κρατών μελών μέσω της ομάδας συνεργασίας στην ανταλλαγή βέλτιστων πρακτικών· διευκόλυνση της δημιουργίας κέντρων κοινοχρησίας και ανάλυσης πληροφοριών (ISAC) ανά τομέα.

Υποστήριξη της επιχειρησιακής συνεργασίας και της διαχείρισης κρίσεων – υποστήριξη της συνεργασίας μεταξύ των αρμόδιων δημόσιων αρχών και των άμεσα ενδιαφερομένων μέσα από την εδραίωση συστηματικής συνεργασίας με τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης που δραστηριοποιούνται στους τομείς της ασφάλειας στον κυβερνοχώρο, του ηλεκτρονικού εγκλήματος και της προστασίας της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα· παροχή γραμματειακής υποστήριξης στο δίκτυο CSIRT (άρθρο 12 παράγραφος 2 (ΕΕ) της οδηγίας 2016/1148) καθώς και συμβολή στην επιχειρησιακή συνεργασία με το δίκτυο με παροχή υποστήριξης, σε συνεργασία με τη CERT-EU, στα κράτη μέλη, κατόπιν αιτήματός τους· διοργάνωση τακτικών ασκήσεων ασφάλειας στον κυβερνοχώρο· συμβολή στην ανάπτυξη κοινής αντιμετώπισης των μεγάλης κλίμακας διασυνοριακών συμβάντων και κρίσεων που αφορούν την ασφάλεια στον κυβερνοχώρο· διεξαγωγή, σε συνεργασία με το δίκτυο

[44] Ως διαφάνεια της διασφάλισης της ασφάλειας στον κυβερνοχώρο ορίζεται η παροχή στους χρήστες επαρκών πληροφοριών σχετικά με τις ιδιότητες ασφάλειας στον κυβερνοχώρο, γεγονός που επιτρέπει στους χρήστες να προσδιορίσουν με αντικειμενικό τρόπο το επίπεδο ασφάλειας ενός δεδομένου προϊόντος, υπηρεσίας ή διαδικασίας ΤΠΕ.

CSIRT, εκ των υστέρων τεχνικών ερευνών για τα σημαντικά συμβάντα και έκδοση συστάσεων παρακολούθησης·

καθήκοντα σχετικά με την αγορά (τυποποίηση, πιστοποίηση) - εκτέλεση μιας σειράς λειτουργιών για τη στήριξη, ειδικότερα, της εσωτερικής αγοράς: «παρατηρητήριο αγοράς» για την ασφάλεια στον κυβερνοχώρο, μέσω της ανάλυσης των σχετικών τάσεων στην αγορά της ασφάλειας στον κυβερνοχώρο ώστε να υπάρχει μεγαλύτερη αντιστοιχία ζήτησης και προσφοράς· υποστήριξη και προώθηση της εκπόνησης και εφαρμογής της ενωσιακής πολιτικής σχετικά με την πιστοποίηση της ασφάλειας στον κυβερνοχώρο των προϊόντων και υπηρεσιών ΤΠΕ, μέσω της επεξεργασίας υποψήφιων ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο, της παροχής γραμματειακής υποστήριξης στην ευρωπαϊκή ομάδα πιστοποίησης της ασφάλειας στον κυβερνοχώρο, της παροχής κατευθυντήριων γραμμών και ορθών πρακτικών σε σχέση με τις απαιτήσεις ασφαλείας των προϊόντων και υπηρεσιών ΤΠΕ σε συνεργασία με τις εθνικές εποπτικές αρχές πιστοποίησης και τους φορείς του κλάδου· **Ενίσχυση των γνώσεων και των πληροφοριών και στήριξη της ευαισθητοποίησης** – παροχή συνδρομής και συμβουλών στην Επιτροπή και στα κράτη μέλη προκειμένου να επιτύχουν ένα υψηλό επίπεδο γνώσεων, σε ολόκληρη την Ένωση, επί θεμάτων που σχετίζονται με την ασφάλεια δικτύων και πληροφοριών και την εφαρμογή της στις επιχειρήσεις του κλάδου. Εδώ εντάσσεται επίσης η συγκέντρωση, οργάνωση και διάθεση στο κοινό, μέσω ειδικής δικτυακής πύλης, πληροφοριών σχετικά με την ασφάλεια των συστημάτων δικτύου ή πληροφοριών [ή την ασφάλεια στον κυβερνοχώρο]. Άλλη σημαντική πτυχή αποτελούν οι δραστηριότητες ευαισθητοποίησης και οι εκστρατείες προβολής που απευθύνονται στο ευρύ κοινό σχετικά με τους κινδύνους για την ασφάλεια στον κυβερνοχώρο.

Ενίσχυση της στήριξης στην έρευνα και καινοτομία - παροχή συμβουλών σχετικά με τις ερευνητικές ανάγκες και τον καθορισμό των ερευνητικών προτεραιοτήτων στον τομέα της ασφάλειας στον κυβερνοχώρο.

Ενίσχυση της διεθνούς συνεργασίας – υποστήριξη των προσπαθειών της Ένωσης για συνεργασία με τρίτες χώρες και διεθνείς οργανισμούς για την προώθηση της διεθνούς συνεργασίας σε σχέση με την ασφάλεια στον κυβερνοχώρο.

ΠΙΣΤΟΠΟΙΗΣΗ

Το **πλαίσιο πιστοποίησης θα συμβάλει στην επίτευξη των στόχων** αυξάνοντας τη συνολική διαφάνεια της διασφάλισης της ασφάλειας στον κυβερνοχώρο[45] για τα προϊόντα και τις υπηρεσίες ΤΠΕ και, ως εκ τούτου, ενισχύοντας την εμπιστοσύνη στην ψηφιακή ενιαία αγορά και στην ψηφιακή καινοτομία. Αναμένεται να συμβάλει επίσης στην αποφυγή του κατακερματισμού των συστημάτων πιστοποίησης στην ΕΕ και των σχετικών απαιτήσεων ασφαλείας και κριτηρίων αξιολόγησης στα κράτη μέλη και τους διάφορους τομείς.

1.4.3. Αναμενόμενο(-α) αποτέλεσμα(-τα) και επιπτώσεις

Να προσδιοριστούν τα αποτελέσματα που θα πρέπει να έχει η πρόταση/πρωτοβουλία όσον αφορά τους(τις) στοχοθετημένους(-ες) δικαιούχους/ομάδες.

Ένας αναβαθμισμένος ENISA (που θα υποστηρίζει τις ικανότητες, την πρόληψη, τη συνεργασία και την ευαισθητοποίηση σε επίπεδο ΕΕ με στόχο την ενίσχυση της συνολικής

[45] Ως διαφάνεια της διασφάλισης της ασφάλειας στον κυβερνοχώρο ορίζεται η παροχή στους χρήστες επαρκών πληροφοριών σχετικά με τις ιδιότητες ασφάλειας στον κυβερνοχώρο, γεγονός που επιτρέπει στους χρήστες να προσδιορίσουν με αντικειμενικό τρόπο το επίπεδο ασφάλειας ενός δεδομένου προϊόντος, υπηρεσίας ή διαδικασίας ΤΠΕ.

ανθεκτικότητας της ΕΕ στον κυβερνοχώρο), καθώς και η υποστήριξη του ενωσιακού πλαισίου πιστοποίησης των προϊόντων και υπηρεσιών ΤΠΕ προσδοκάται ότι θα έχει τις ακόλουθες επιπτώσεις (μη εξαντλητικός κατάλογος):

Συνολικές επιπτώσεις:

- Συνολικός θετικός αντίκτυπος στην εσωτερική αγορά χάρη στον περιορισμό του κατακερματισμού της αγοράς και την ανάπτυξη της εμπιστοσύνης στις ψηφιακές τεχνολογίες μέσω καλύτερης συνεργασίας, πιο εναρμονισμένων προσεγγίσεων των ενωσιακών πολιτικών ασφάλειας στον κυβερνοχώρο και αυξημένων ικανοτήτων σε επίπεδο ΕΕ. Αυτό προσδοκάται ότι θα έχει θετικό οικονομικό αντίκτυπο συμβάλλοντας στη μείωση του κόστους των συμβάντων που αφορούν την ασφάλεια στον κυβερνοχώρο/το ηλεκτρονικό έγκλημα, το οποίο εκτιμάται ότι ανέρχεται στην Ένωση σε 0,41% του ΑΕΠ της ΕΕ (δηλαδή γύρω στα 55 δισ. ευρώ).

Ειδικά αποτελέσματα:

Βελτιωμένες ικανότητες και ετοιμότητα των κρατών μελών και των επιχειρήσεων όσον αφορά την ασφάλεια στον κυβερνοχώρο

- Βελτιωμένες ικανότητες και ετοιμότητα των κρατών μελών όσον αφορά την ασφάλεια στον κυβερνοχώρο (μέσα από τη μακροπρόθεσμη στρατηγική ανάλυση των απειλών και των συμβάντων στον κυβερνοχώρο, την παροχή κατευθύνσεων και την υποβολή εκθέσεων, τη μεσιτεία εμπειρογνωσίας και ορθών πρακτικών, την εκπαίδευση και τη διαθεσιμότητα εκπαιδευτικού υλικού, την ενίσχυση των ασκήσεων CyberEurope)

- Βελτιωμένες ικανότητες των ιδιωτικών φορέων χάρη στην υποστήριξη της σύστασης κέντρων κοινοχρησίας και ανάλυσης πληροφοριών (ISAC) σε διάφορους τομείς.

- Βελτιωμένη ετοιμότητα της ΕΕ και των κρατών μελών όσον αφορά την ασφάλεια στον κυβερνοχώρο χάρη στη διαθεσιμότητα καλά προετοιμασμένων και συμφωνημένων σχεδίων, τα οποία έχουν δοκιμαστεί στις ασκήσεις CyberEurope, σε περίπτωση μεγάλης κλίμακας διασυνοριακού συμβάντος που αφορά την ασφάλεια στον κυβερνοχώρο.

Βελτιωμένη συνεργασία και συντονισμός στα κράτη μέλη και τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ

- Βελτιωμένη συνεργασία τόσο στους κόλπους όσο και μεταξύ του δημόσιου και του ιδιωτικού τομέα.

- Πιο συνεκτική προσέγγιση όσον αφορά την εφαρμογή της οδηγίας για την ασφάλεια δικτύου και πληροφοριών (NIS) σε διασυνοριακή κλίμακα και στους διάφορους τομείς.

- Βελτίωση της συνεργασίας στον τομέα της πιστοποίησης χάρη σε ένα θεσμικό πλαίσιο που θα επιτρέπει την ανάπτυξη ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο και τη χάραξη κοινής πολιτικής στον τομέα αυτό.

Αυξημένες ικανότητες σε επίπεδο ΕΕ για τη συμπλήρωση της δράσης των κρατών μελών

- Βελτίωση της «επιχειρησιακής ικανότητας της ΕΕ» με σκοπό τη συμπλήρωση της δράσης των κρατών μελών και την υποστήριξή τους κατόπιν σχετικού αιτήματος και σε σχέση με περιορισμένες και προκαθορισμένες υπηρεσίες· Αυτό αναμένεται ότι θα έχει θετικό αντίκτυπο στην επιτυχία της πρόληψης, του εντοπισμού και της ικανότητας αντιμετώπισης των συμβάντων τόσο σε επίπεδο κρατών μελών όσο και σε επίπεδο Ένωσης·

Αυξημένη ευαισθητοποίηση των πολιτών και των επιχειρήσεων σε ζητήματα ασφάλειας στον κυβερνοχώρο

- Μεγαλύτερη εν γένει ευαισθητοποίηση των πολιτών και των επιχειρήσεων σε ζητήματα ασφάλειας στον κυβερνοχώρο

- Μεγαλύτερη ικανότητα για λήψη τεκμηριωμένων αποφάσεων αγοράς σε σχέση με τα προϊόντα και τις υπηρεσίες ΤΠΕ χάρη στην πιστοποίηση της ασφάλειας στον κυβερνοχώρο

Ενισχυμένη εμπιστοσύνη στην ψηφιακή ενιαία αγορά και στην ψηφιακή καινοτομία μέσα από την αυξημένη διαφάνεια της διασφάλισης της ασφάλειας στον κυβερνοχώρο των προϊόντων και υπηρεσιών ΤΠΕ

- Αυξημένη διαφάνεια της διασφάλισης της ασφάλειας στον κυβερνοχώρο[46] των προϊόντων και υπηρεσιών ΤΠΕ χάρη στην απλοποίηση των διαδικασιών για την πιστοποίηση της ασφαλείας μέσω πλαισίου σε επίπεδο ΕΕ

- Υψηλότερο επίπεδο διασφάλισης των ιδιοτήτων ασφαλείας των προϊόντων και υπηρεσιών ΤΠΕ

- Αυξημένη χρήση της πιστοποίησης ασφάλειας χάρη στην παροχή κινήτρων μέσω απλουστευμένων διαδικασιών, μείωσης του κόστους και προοπτικών για επιχειρηματικές ευκαιρίες σε ολόκληρη την ΕΕ χωρίς εμπόδια λόγω κατακερματισμού της αγοράς

- Βελτίωση της ανταγωνιστικότητας στην αγορά της ασφάλειας στον κυβερνοχώρο χάρη στη μείωση του κόστους και της διοικητικής επιβάρυνσης για τις ΜΜΕ και στην κατάργηση πιθανών εμποδίων για την είσοδο στην αγορά λόγω των πολυάριθμων εθνικών συστημάτων πιστοποίησης

Άλλα

- Δεν αναμένονται σημαντικές περιβαλλοντικές επιπτώσεις για κανέναν από τους στόχους.

- Όσον αφορά τον προϋπολογισμό της ΕΕ, αναμένεται βελτίωση της αποτελεσματικότητας χάρη στη βελτίωση της συνεργασίας και του συντονισμού των δραστηριοτήτων μεταξύ των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης.

1.4.4. Δείκτες αποτελεσμάτων και επιπτώσεων

Να προσδιοριστούν οι δείκτες για την παρακολούθηση της υλοποίησης της πρότασης/πρωτοβουλίας.

α)

Στόχος: Αύξηση των ικανοτήτων και της ετοιμότητας των κρατών μελών και των επιχειρήσεων:

- Αριθμός εκπαιδεύσεων που οργανώθηκαν από τον ENISA
- Γεωγραφική κάλυψη (αριθμός χωρών και περιοχών) της άμεσης συνδρομής που παρέχει ο ENISA
- Επίπεδο ετοιμότητας στο οποίο έχουν φτάσει τα κράτη μέλη όσον αφορά την ωριμότητα των CSIRT και την επίβλεψη των κανονιστικών μέτρων που

[46] Ως διαφάνεια της διασφάλισης της ασφάλειας στον κυβερνοχώρο ορίζεται η παροχή στους χρήστες επαρκών πληροφοριών σχετικά με τις ιδιότητες ασφάλειας στον κυβερνοχώρο, γεγονός που επιτρέπει στους χρήστες να προσδιορίσουν με αντικειμενικό τρόπο το επίπεδο ασφάλειας ενός δεδομένου προϊόντος, υπηρεσίας ή διαδικασίας ΤΠΕ.

σχετίζονται με την ασφάλεια στον κυβερνοχώρο

- Αριθμός ορθών πρακτικών σε επίπεδο ΕΕ για τις υποδομές κρίσιμης σημασίας που παρέχονται από τον ENISA
- Αριθμός ορθών πρακτικών σε επίπεδο ΕΕ για ΜΜΕ που παρέχονται από τον ENISA
- Δημοσίευση ετήσιας στρατηγικής ανάλυσης των απειλών και των συμβάντων στον κυβερνοχώρο με στόχο των προσδιορισμό των αναδυόμενων τάσεων από τον ENISA
- Τακτική συμβολή του ENISA στο έργο των ομάδων εργασίας για την ασφάλεια στον κυβερνοχώρο των ευρωπαϊκών οργανισμών τυποποίησης

Στόχος: Βελτίωση της συνεργασίας και του συντονισμού μεταξύ των κρατών μελών και των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ:

- Αριθμός κρατών μελών που χρησιμοποίησαν τις συστάσεις και τις γνωμοδοτήσεις του ENISA στην οικεία διαδικασία χάραξης πολιτικής
- Αριθμός θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ που χρησιμοποίησαν τις συστάσεις και τις γνωμοδοτήσεις του ENISA στη διαδικασία χάραξης της πολιτικής τους
- Κανονική υλοποίηση του προγράμματος εργασιών του δικτύου CSIRT και εύρυθμη λειτουργία της υποδομής ΤΠ και των διαύλων επικοινωνίας του δικτύου CSIRT
- Αριθμός τεχνικών εκθέσεων που διατέθηκαν στην ομάδα συνεργασίας και χρησιμοποιήθηκαν από αυτή
- Συνεκτική προσέγγιση της εφαρμογής της οδηγίας NIS σε διασυνοριακή κλίμακα και στους διάφορους τομείς
- Αριθμός αξιολογήσεων κανονιστικής συμμόρφωσης που διενήργησε ο ENISA
- Αριθμός ISAC που συστήθηκαν στους διάφορους τομείς, ιδίως για τις υποδομές κρίσιμης σημασίας
- Δημιουργία και κανονική λειτουργία πλατφόρμας πληροφοριών για τη διάχυση πληροφοριών σχετικά με την ασφάλεια στον κυβερνοχώρο οι οποίες προέρχονται από τα θεσμικά και λοιπά όργανα και οργανισμούς της ΕΕ
- Τακτική συμβολή στην κατάρτιση των προγραμμάτων εργασιών έρευνας και καινοτομίας της ΕΕ
- Σύναψη συμφωνίας συνεργασίας μεταξύ ENISA, EC3 και CERT-EU
- Αριθμός συστημάτων πιστοποίησης που περιλαμβάνονται και αναπτύσσονται βάσει του πλαισίου

Στόχος: Αύξηση των ικανοτήτων σε επίπεδο ΕΕ για τη συμπλήρωση της δράσης των κρατών μελών, ιδίως στην περίπτωση των διασυνοριακών κρίσεων στον κυβερνοχώρο:

- Δημοσίευση ετήσιας στρατηγικής ανάλυσης των απειλών και των συμβάντων στον κυβερνοχώρο με στόχο των προσδιορισμό των αναδυόμενων τάσεων από τον ENISA
- Δημοσίευση συγκεντρωτικών πληροφοριών σχετικά με τα συμβάντα που καταγγέλλονται σύμφωνα με την οδηγία NIS από τον ENISA

- Αριθμός πανευρωπαϊκών ασκήσεων που συντονίστηκαν από τον Οργανισμό και αριθμός συμμετεχόντων κρατών μελών και οργανισμών
- Αριθμός αιτημάτων για υποστήριξη στην αντιμετώπιση έκτακτων καταστάσεων από κράτη μέλη προς τον ENISA και αριθμός αιτημάτων στα οποία ανταποκρίθηκε
- Αριθμός αναλύσεων τρωτών σημείων, σφαλμάτων και συμβάντων που πραγματοποιήθηκαν από τον ENISA σε συνεργασία με την CERT-EU.
- Διαθεσιμότητα εκθέσεων κατάστασης για ολόκληρη την ΕΕ με βάση τις πληροφορίες που διατίθενται στον ENISA από τα κράτη μέλη και από άλλους φορείς σε περίπτωση διασυνοριακού συμβάντος μεγάλης κλίμακας στον κυβερνοχώρο.

Στόχος: Αυξημένη ευαισθητοποίηση των πολιτών και των επιχειρήσεων σε ζητήματα ασφάλειας στον κυβερνοχώρο:

- Τακτική διεξαγωγή εκστρατειών ευαισθητοποίησης σε επίπεδο ΕΕ και σε εθνικό επίπεδο και τακτική επικαιροποίηση των θεμάτων σύμφωνα με τις αναδυόμενες μαθησιακές ανάγκες.
- Ενίσχυση της ευαισθητοποίησης των πολιτών της ΕΕ σχετικά με τον κυβερνοχώρο.
- Τακτική διεξαγωγή του τεστ ευαισθητοποίησης σε ζητήματα ασφάλειας στον κυβερνοχώρο και αύξηση των σωστών απαντήσεων σε βάθος χρόνου.
- Τακτική δημοσίευση ορθών πρακτικών σε σχέση με την ασφάλεια στον κυβερνοχώρο και την κυβερνοϋγιεινή.

Στόχος: Ενίσχυση της εμπιστοσύνης στην ψηφιακή ενιαία αγορά και την ψηφιακή καινοτομία μέσα από την αύξηση της συνολικής διαφάνειας της διασφάλισης της ασφάλειας στον κυβερνοχώρο[47] των προϊόντων και υπηρεσιών ΤΠΕ:

- Αριθμός συστημάτων που εντάσσονται στο πλαίσιο της ΕΕ
- Μειωμένο κόστος χορήγησης πιστοποιητικού ασφάλειας ΤΠΕ
- Αριθμός οργανισμών αξιολόγησης της συμμόρφωσης με ειδίκευση στην πιστοποίηση ΤΠΕ στα κράτη μέλη
- Σύσταση της ευρωπαϊκής ομάδας πιστοποίησης της ασφάλειας στον κυβερνοχώρο και τακτική σύγκληση συνεδριάσεων
- Κατευθυντήριες γραμμές για την πιστοποίηση σύμφωνα με το ισχύον πλαίσιο της ΕΕ
- Τακτική δημοσίευση αναλύσεων των βασικών τάσεων στην αγορά της ασφάλειας στον κυβερνοχώρο της ΕΕ
- Αριθμός πιστοποιημένων προϊόντων και υπηρεσιών ΤΠΕ σύμφωνα με τους κανόνες του ευρωπαϊκού πλαισίου πιστοποίησης της ασφάλειας ΤΠΕ
- Αυξημένος αριθμός τελικών χρηστών που είναι ενημερωμένοι για τα

[47] Ως διαφάνεια της διασφάλισης της ασφάλειας στον κυβερνοχώρο ορίζεται η παροχή στους χρήστες επαρκών πληροφοριών σχετικά με τις ιδιότητες ασφάλειας στον κυβερνοχώρο, γεγονός που επιτρέπει στους χρήστες να προσδιορίσουν με αντικειμενικό τρόπο το επίπεδο ασφάλειας ενός δεδομένου προϊόντος, υπηρεσίας ή διαδικασίας ΤΠΕ.

χαρακτηριστικά ασφαλείας των προϊόντων και υπηρεσιών ΤΠΕ

β)

1.4.5. Βραχυπρόθεσμη ή μακροπρόθεσμη κάλυψη αναγκών

Υπό το φως των κανονιστικών απαιτήσεων και της ταχέως εξελισσόμενης φύσης των απειλών για την ασφάλεια στον κυβερνοχώρο, η εντολή του ENISA πρέπει να επανεξεταστεί προκειμένου να καθοριστεί ανανεωμένη σειρά καθηκόντων και λειτουργιών, με σκοπό την αποτελεσματική και αποδοτική υποστήριξη των κρατών μελών, των θεσμικών οργάνων της ΕΕ και των προσπαθειών άλλων άμεσα ενδιαφερόμενων για τη διασφάλιση ασφαλούς κυβερνοχώρου στην Ευρωπαϊκή Ένωση. Οριοθετείται το προτεινόμενο εύρος της εντολής, που ενισχύει τους τομείς στους οποίους είναι σαφές ότι ο Οργανισμός παράγει προστιθέμενη αξία και προσθέτει εκείνους τους νέους τομείς που χρήζουν στήριξης με βάση τις νέες προτεραιότητες και μέσα πολιτικής, συγκεκριμένα την οδηγία NIS, την επανεξέταση της Στρατηγικής της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο, το προσχέδιο της ΕΕ για την ασφάλεια στον κυβερνοχώρο εν όψει της συνεργασίας στην αντιμετώπιση των κρίσεων στον κυβερνοχώρο, και την πιστοποίηση ασφαλείας ΤΠΕ. Στόχος της νέας προτεινόμενης εντολής είναι να προσδώσει στον Οργανισμό ισχυρότερο και πιο κεντρικό ρόλο, κυρίως με την πιο ενεργή στήριξη και των κρατών μελών στην αντιμετώπιση συγκεκριμένων απειλών (επιχειρησιακή ικανότητα) και με τη μετατροπή του σε κέντρο εμπειρογνωσίας για τη στήριξη των κρατών μελών και της Επιτροπής σε θέματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο. Παράλληλα, η πρόταση καθιερώνει ευρωπαϊκό πλαίσιο πιστοποίησης της ασφάλειας στον κυβερνοχώρο για τα προϊόντα και τις υπηρεσίες ΤΠΕ και καθορίζει τις βασικές λειτουργίες και καθήκοντα του ENISA στον τομέα της πιστοποίησης της ασφάλειας στον κυβερνοχώρο. Το πλαίσιο καθορίζει κοινές διατάξεις και διαδικασίες που επιτρέπουν τη δημιουργία συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο σε επίπεδο ΕΕ για συγκεκριμένα προϊόντα/υπηρεσίες ΤΠΕ ή κινδύνους για την ασφάλεια στον κυβερνοχώρο. Η δημιουργία ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο σύμφωνα με το πλαίσιο θα επιτρέψει την έκδοση πιστοποιητικών βάσει των εν λόγω συστημάτων τα οποία θα είναι έγκυρα και αναγνωρισμένα σε όλα τα κράτη μέλη, και την αντιμετώπιση του σημερινού κατακερματισμού της αγοράς.

1.4.6. Προστιθέμενη αξία παρέμβασης της ΕΕ

Η ασφάλεια στον κυβερνοχώρο είναι ένα πραγματικά παγκόσμιο πρόβλημα διασυνοριακής κλίμακας το οποίο αποκτά όλο και περισσότερο διατομεακό χαρακτήρα λόγω των αλληλεξαρτήσεων μεταξύ των δικτύων και των πληροφοριακών συστημάτων. Ο αριθμός, η πολυπλοκότητα και η κλίμακα των συμβάντων που αφορούν την ασφάλεια στον κυβερνοχώρο και οι επιπτώσεις τους στην οικονομία αυξάνονται με το πέρασμα του χρόνου και αναμένεται να αυξηθούν ακόμη περισσότερο παράλληλα με τις τεχνολογικές εξελίξεις, π.χ. την ανάπτυξη του διαδικτύου των πραγμάτων. Αυτό συνεπάγεται ότι η ανάγκη για αυξημένη κοινή προσπάθεια από τα κράτη μέλη, τα όργανα της ΕΕ και άμεσα ενδιαφερόμενους από τον ιδιωτικό τομέα με στόχο την αντιμετώπιση των απειλών για την ασφάλεια στον κυβερνοχώρο δεν πρόκειται να αμβλυνθεί στο μέλλον. Από την ίδρυσή του το 2004, ο ENISA επιδιώκει να ενθαρρύνει τη συνεργασία μεταξύ των κρατών μελών και των άμεσα ενδιαφερομένων για την ασφάλεια δικτύου και

πληροφοριών (NIS), συμπεριλαμβανομένης της στήριξης της συνεργασίας δημόσιου-ιδιωτικού τομέα. Αυτή η στήριξη της συνεργασίας περιλάμβανε την τεχνική εργασία για την παροχή μιας πανευρωπαϊκής εικόνας της φύσης των απειλών, τη σύσταση ομάδων εμπειρογνωμόνων και τη διοργάνωση πανευρωπαϊκών ασκήσεων διαχείρισης συμβάντων και κρίσεων για τον δημόσιο και ιδιωτικό τομέα (πιο συγκεκριμένα της «Cyber Europe»). Η οδηγία NIS ανέθεσε στον ENISA πρόσθετα καθήκοντα, συμπεριλαμβανομένης της γραμματειακής υποστήριξης του δικτύου CSIRT για την επιχειρησιακή συνεργασία μεταξύ των κρατών μελών.

Η προστιθέμενη αξία της δράσης σε επίπεδο ΕΕ, ιδίως για την ενίσχυση της συνεργασίας μεταξύ των κρατών μελών αλλά και μεταξύ των κοινοτήτων NIS αναγνωρίστηκε από τα συμπεράσματα του Συμβουλίου του 2016[48] και προκύπτει επίσης ξεκάθαρα από την αξιολόγηση του ENISA για το 2017, όπου φαίνεται ότι η προστιθέμενη αξία του Οργανισμού έγκειται πρωτίστως στην ικανότητά του να ενισχύει τη συνεργασία μεταξύ αυτών των άμεσα ενδιαφερομένων. Δεν υπάρχει άλλος φορέας σε επίπεδο ΕΕ που να στηρίζει τη συνεργασία ενός τέτοιου εύρους άμεσα ενδιαφερομένων στο πεδίο της ασφάλειας των δικτύων και των πληροφοριών (NIS).

Η προστιθέμενη αξία του ENISA όσον αφορά την ενθάρρυνση της συνεργασίας των κοινοτήτων και των άμεσα ενδιαφερομένων για την ασφάλεια στον κυβερνοχώρο ισχύει επίσης στον τομέα της πιστοποίησης. Η αύξηση του ηλεκτρονικού εγκλήματος και των απειλών για την ασφάλεια στον κυβερνοχώρο είχε ως αποτέλεσμα την ανάληψη εθνικών πρωτοβουλιών οι οποίες θέσπισαν υψηλές απαιτήσεις πιστοποίησης και ασφάλειας στον κυβερνοχώρο για τα στοιχεία ΤΠΕ που χρησιμοποιούνται στις παραδοσιακές υποδομές. Αν και σημαντικές, οι πρωτοβουλίες αυτές ενέχουν τον κίνδυνο του κατακερματισμού της ενιαίας αγοράς και της δημιουργίας εμποδίων στη διαλειτουργικότητα. Ένας πωλητής ΤΠΕ μπορεί να χρειαστεί να υποβληθεί σε σειρά διαδικασιών πιστοποίησης προκειμένου να μπορεί να πωλεί τα προϊόντα του σε περισσότερα κράτη μέλη. Η αναποτελεσματικότητα/έλλειψη αποδοτικότητας των τρεχόντων συστημάτων πιστοποίησης είναι μάλλον απίθανο να λυθεί χωρίς παρέμβαση της ΕΕ. Αν δεν αναληφθεί δράση, ο κατακερματισμός της αγοράς είναι πολύ πιθανό να οξυνθεί σε βραχυπρόθεσμο-μεσοπρόθεσμο επίπεδο (μέσα στα επόμενα 5-10 χρόνια) με την ανάδυση νέων συστημάτων πιστοποίησης. Η απουσία συντονισμού και διαλειτουργικότητας μεταξύ αυτών των συστημάτων είναι ένα στοιχείο που υπονομεύει τις δυνατότητες της ψηφιακής ενιαίας αγοράς. Αυτό καταδεικνύει την προστιθέμενη αξία της καθιέρωσης ενός ευρωπαϊκού πλαισίου πιστοποίησης της ασφάλειας στον κυβερνοχώρο για τα προϊόντα και τις υπηρεσίες ΤΠΕ το οποίο θεσπίζει τις κατάλληλες προϋποθέσεις για την αποτελεσματική αντιμετώπιση του προβλήματος που σχετίζεται με την ταυτόχρονη ύπαρξη πολλών διαδικασιών πιστοποίησης στα διάφορα κράτη μέλη, μειώνει το κόστος πιστοποίησης καθιστώντας έτσι την πιστοποίηση στην ΕΕ συνολικά πιο ελκυστική από εμπορική σκοπιά και από τη σκοπιά του ανταγωνισμού.

1.4.7. Διδάγματα που αποκομίστηκαν από ανάλογες εμπειρίες του παρελθόντος

Σύμφωνα με τη νομική βάση του ENISA, η Επιτροπή έχει διενεργήσει αξιολόγηση του Οργανισμού η οποία περιλάμβανε ανεξάρτητη μελέτη καθώς και δημόσια διαβούλευση. Η αξιολόγηση κατέληξε στο συμπέρασμα ότι οι στόχοι του ENISA παραμένουν σήμερα επίκαιροι . Σε ένα πλαίσιο τεχνολογικών εξελίξεων και εξελισσόμενων απειλών και,

[48] Συμπεράσματα του Συμβουλίου σχετικά με την ενίσχυση του ευρωπαϊκού συστήματος ανθεκτικότητας στον κυβερνοχώρο και την προώθηση ενός ανταγωνιστικού και καινοτόμου κλάδου κυβερνοασφάλειας - 15 Νοεμβρίου 2016.

ταυτόχρονα, μεγάλης ανάγκης για αυξημένη ασφάλεια των δικτύων και των πληροφοριών (NIS) στην ΕΕ, απαιτείται τεχνική εμπειρογνωσία στην εξέλιξη των θεμάτων ασφάλειας δικτύων και πληροφοριών. Είναι απαραίτητη η οικοδόμηση ικανοτήτων στα κράτη μέλη για την κατανόηση και την αντιμετώπιση των απειλών και η συνεργασία των άμεσα ενδιαφερόμενων μεταξύ θεματικών πεδίων και οργανισμών.

Ο οργανισμός συνέβαλε επιτυχώς στη βελτίωση της ασφάλειας των δικτύων και των πληροφοριών (NIS) στην Ευρώπη μέσω της προσφοράς ανάπτυξης ικανοτήτων στα 28 κράτη μέλη, της ενίσχυσης της συνεργασίας μεταξύ κρατών μελών και άμεσα ενδιαφερόμενων για την ασφάλεια δικτύων και πληροφοριών, και μέσω της παροχής εμπειρογνωσίας, ανάπτυξης κοινότητας και υποστήριξης για την ανάπτυξη πολιτικών.

Αν και ο ENISA κατάφερε να έχει αντίκτυπο, τουλάχιστον σε ορισμένο βαθμό, στο ευρύ πεδίο της ασφάλειας δικτύων και πληροφοριών, ωστόσο δεν έχει πετύχει απόλυτα στην ανάπτυξη ισχυρής επωνυμίας και την εξασφάλιση επαρκούς προβολής ώστε να είναι αναγνωρίσιμος ως το βασικό κέντρο εμπειρογνωσίας στην Ευρώπη. Αυτό οφείλεται στο εύρος της εντολής του ENISA, που όμως δεν συνοδεύτηκε με αντίστοιχα σημαντικούς πόρους. Επιπλέον, ο ENISA παραμένει ο μοναδικός οργανισμός της ΕΕ με εντολή καθορισμένου χρόνου, γεγονός που περιορίζει την ικανότητά του να αναπτύξει μακροπρόθεσμο όραμα και να υποστηρίξει τους άμεσα ενδιαφερόμενους κατά τρόπο βιώσιμο. Αυτό έρχεται επίσης σε αντίθεση με τις διατάξεις της οδηγίας NIS που επιφορτίζουν τον ENISA με καθήκοντα χωρίς καταληκτική ημερομηνία.

Όσον αφορά την πιστοποίηση της ασφάλειας στον κυβερνοχώρο για τα προϊόντα και τις υπηρεσίες ΤΠΕ, αυτή τη στιγμή δεν υπάρχει ευρωπαϊκό πλαίσιο. Ωστόσο, η αύξηση του ηλεκτρονικού εγκλήματος και των απειλών για την ασφάλεια στον κυβερνοχώρο είχε ως αποτέλεσμα την ανάληψη εθνικών πρωτοβουλιών, οι οποίες δημιουργούν κίνδυνο κατακερματισμού της ενιαίας αγοράς.

1.4.8. Συμβατότητα και ενδεχόμενη συνέργεια με άλλα κατάλληλα μέσα

Η πρωτοβουλία είναι καθ' όλα συμβατή με τις υφιστάμενες πολιτικές, ειδικά στον τομέα της εσωτερικής αγοράς. Πράγματι, σχεδιάστηκε σύμφωνα με τη συνολική προσέγγιση της ασφάλειας στον κυβερνοχώρο, όπως καθορίστηκε από την επανεξέταση της στρατηγικής για την ψηφιακή ενιαία αγορά, με σκοπό να λειτουργήσει συμπληρωματικά σε μια ολοκληρωμένη δέσμη μέτρων, όπως η επανεξέταση της εφαρμογής της Στρατηγικής της ΕΕ για την ασφάλεια στον κυβερνοχώρο, το προσχέδιο για συνεργασία στην αντιμετώπιση των κρίσεων στον κυβερνοχώρο και οι πρωτοβουλίες για την καταπολέμηση του ηλεκτρονικού εγκλήματος. Αναμένεται ότι θα συμβάλει στην ευθυγράμμιση με, και ότι θα αξιοποιήσει, τις διατάξεις της υφιστάμενης νομοθεσίας, ιδίως δε της οδηγίας NIS, με στόχο τη ενίσχυση της ανθεκτικότητας της ΕΕ στον κυβερνοχώρο μέσω της βελτίωσης των ικανοτήτων, της συνεργασίας, της διαχείρισης των κινδύνων και της ευαισθητοποίησης στα θέματα του κυβερνοχώρου.

Τα προτεινόμενα μέτρα πιστοποίησης αναμένεται ότι θα αντιμετωπίσουν τον πιθανό κατακερματισμό που προκαλείται από τα υφιστάμενα και τα νεοεμφανιζόμενα εθνικά συστήματα πιστοποίησης, συμβάλλοντας έτσι στην ανάπτυξη της ψηφιακής ενιαίας αγοράς. Επίσης, η πρωτοβουλία στηρίζει και συμπληρώνει την εφαρμογή της οδηγίας NIS παρέχοντας στις επιχειρήσεις που εμπίπτουν στην οδηγία ένα εργαλείο για την απόδειξη της συμμόρφωσης με τις απαιτήσεις NIS σε ολόκληρη την Ένωση.

Το προτεινόμενο ευρωπαϊκό πλαίσιο πιστοποίησης της ασφάλειας στον κυβερνοχώρο για την ΤΠΕ, δεν επηρεάζει τον γενικό κανονισμό για την προστασία δεδομένων (ΓΚΠΔ)[49] και ειδικότερα τις σχετικές διατάξεις για την πιστοποίηση[50] όπως ισχύουν για την ασφάλεια της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Τέλος, στο μέτρο του δυνατού, τα συστήματα που θα προταθούν στο μελλοντικό ευρωπαϊκό πλαίσιο θα πρέπει να βασίζονται στα διεθνή πρότυπα σε μια προσπάθεια να αποφευχθεί η δημιουργία εμπορικών φραγμών και να διασφαλιστεί η συνοχή με τις διεθνείς πρωτοβουλίες.

1.5. Διάρκεια και δημοσιονομικές επιπτώσεις

☐ Πρόταση/πρωτοβουλία **περιορισμένης διάρκειας**

– ☐ Πρόταση/Πρωτοβουλία με ισχύ από την [ΗΗ/ΜΜ]ΕΕΕΕ μέχρι την [ΗΗ/ΜΜ]ΕΕΕΕ

– ☐ Δημοσιονομικές επιπτώσεις από το ΕΕΕΕ έως το ΕΕΕΕ

☒ Πρόταση/πρωτοβουλία **απεριόριστης διάρκειας**

– Περίοδος σταδιακής εφαρμογής από το 2019 έως το 2020

– και στη συνέχεια πλήρης εφαρμογή.

1.6. Προβλεπόμενος(-οι) τρόπος(-οι) διαχείρισης[51]

☒ **Άμεση διαχείριση** από την Επιτροπή (Τίτλος ΙΙΙ – Πιστοποίηση)

– ☐ από τους εκτελεστικούς οργανισμούς

☐ **Επιμερισμένη διαχείριση** με τα κράτη μέλη

☒ **Έμμεση διαχείριση** με ανάθεση εκτελεστικών καθηκόντων σε:

☐ διεθνείς οργανισμούς και τις οργανώσεις τους (να προσδιοριστούν),

☐ την ΕΤΕπ και το Ευρωπαϊκό Ταμείο Επενδύσεων,

☒ τους οργανισμούς που αναφέρονται στα άρθρα 208 και 209 (Τίτλος ΙΙ – ENISA),

☐ οργανισμούς δημοσίου δικαίου,

☐ οργανισμούς που διέπονται από ιδιωτικό δίκαιο με αποστολή δημόσιας υπηρεσίας στον βαθμό που προσφέρουν επαρκείς οικονομικές εγγυήσεις,

☐ οργανισμούς που διέπονται από το ιδιωτικό δίκαιο κράτους μέλους, στους οποίους έχει ανατεθεί η εκτέλεση σύμπραξης δημόσιου και ιδιωτικού τομέα και που προσφέρουν επαρκείς οικονομικές εγγυήσεις,

☐ πρόσωπα επιφορτισμένα με την εκτέλεση συγκεκριμένων δράσεων στην ΚΕΠΠΑ δυνάμει του τίτλου V της ΣΕΕ και προσδιορίζονται στην αντίστοιχη βασική πράξη.

---

49 Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων).

50 Όπως τα άρθρα 42 (Πιστοποίηση) και 43 (Φορείς πιστοποίησης) καθώς και τα άρθρα 57, 58, και 70 σχετικά με τα καθήκοντα και τις εξουσίες των ανεξάρτητων αρχών ελέγχου και τα καθήκοντα του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων αντιστοίχως.

51 Οι λεπτομέρειες σχετικά με τους τρόπους διαχείρισης, καθώς και οι παραπομπές στον δημοσιονομικό κανονισμό είναι διαθέσιμες στον δικτυακό τόπο BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

Παρατηρήσεις

Ο κανονισμός καλύπτει: - ο τίτλος ΙΙ του προτεινόμενου κανονισμού αναθεωρεί την εντολή του Οργανισμού της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) αναβαθμίζοντας τον ρόλο της πιστοποίησης ενώ - ο τίτλος ΙΙΙ θεσπίζει πλαίσιο για τη δημιουργία ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο για τα προϊόντα και τις υπηρεσίες ΤΠΕ, στο οποίο ο ENISA διαδραματίζει καίριο ρόλο.

2. ΜΕΤΡΑ ΔΙΑΧΕΙΡΙΣΗΣ

2.1. Διατάξεις στον τομέα της παρακολούθησης και της υποβολής εκθέσεων

Να προσδιοριστούν η συχνότητα και οι όροι των διατάξεων αυτών

Η παρακολούθηση θα αρχίσει αμέσως μετά την έκδοση του νομικού μέσου και θα εστιάζει στην εφαρμογή του. Η Επιτροπή θα οργανώνει συναντήσεις με τον ENISA, εκπροσώπους των κρατών μελών (π.χ. ομάδες εμπειρογνωμόνων) και τους συναφείς άμεσα ενδιαφερομένους με σκοπό, συγκεκριμένα, τη διευκόλυνση της εφαρμογής των κανόνων που αφορούν την πιστοποίηση, όπως η συγκρότηση του συμβουλίου.

Η πρώτη αξιολόγηση θα διενεργηθεί 5 έτη μετά την έναρξη ισχύος του νομικού μέσου, υπό την προϋπόθεση ότι θα είναι διαθέσιμα επαρκή δεδομένα. Στο νομικό μέσο περιλαμβάνεται συγκεκριμένη ρήτρα αξιολόγησης και αναθεώρησης [άρθρο XXX], βάσει την οποίας η Επιτροπή θα διενεργήσει ανεξάρτητη αξιολόγηση. Η Επιτροπή θα υποβάλει ακολούθως έκθεση στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο σχετικά με τη διενεργηθείσα αξιολόγηση η οποία θα συνοδεύεται, κατά περίπτωση, από πρόταση αναθεώρησης, με στόχο τη μέτρηση του αντίκτυπου του κανονισμού και της προστιθέμενης αξίας του. Περαιτέρω αξιολογήσεις θα διενεργούνται ανά πενταετία. Θα εφαρμόζεται η μεθοδολογία της Επιτροπής για τη βελτίωση της νομοθεσίας σχετικά με την αξιολόγηση. Οι εν λόγω αξιολογήσεις θα διενεργούνται μέσω στοχευμένων συζητήσεων εμπειρογνωμόνων, μελετών και εκτεταμένων διαβουλεύσεων με άμεσα ενδιαφερομένους.

Ο εκτελεστικός διευθυντής του ENISA θα πρέπει να παρουσιάζει στο διοικητικό συμβούλιο αναδρομική αξιολόγηση των δραστηριοτήτων του ENISA ανά διετία. Ο Οργανισμός πρέπει επίσης να εκπονεί σχέδιο δράσης σε συνέχεια των συμπερασμάτων των αναδρομικών αξιολογήσεων και να υποβάλλει κάθε δύο έτη εκθέσεις προόδου στην Επιτροπή. Το διοικητικό συμβούλιο θα πρέπει να επαγρυπνεί για την επαρκή παρακολούθηση της συνέχειας που δίδεται στα εν λόγω συμπεράσματα.

Εικαζόμενα περιστατικά κακοδιοίκησης στις δραστηριότητες του Οργανισμού υπόκεινται σε έρευνες του Ευρωπαίου Διαμεσολαβητή σύμφωνα με τις διατάξεις του άρθρου 228 της Συνθήκης.

Οι πηγές δεδομένων για την προγραμματισμένη παρακολούθηση θα είναι κυρίως ο ENISA, η ευρωπαϊκή ομάδα πιστοποίησης της ασφάλειας στον κυβερνοχώρο, η ομάδα συνεργασίας, το δίκτυο CSIRT και οι αρχές των κρατών μελών. Εκτός από τα δεδομένα που προέρχονται από τις εκθέσεις (συμπεριλαμβανομένων των ετήσιων εκθέσεων δραστηριοτήτων) του ENISA, την ευρωπαϊκή ομάδα πιστοποίησης της ασφάλειας στον κυβερνοχώρο, την ομάδα συνεργασίας και το δίκτυο CSIRT, θα χρησιμοποιούνται, όταν χρειάζεται, ειδικά εργαλεία συλλογής δεδομένων (π.χ. έρευνες στις εθνικές αρχές, το Ευρωβαρόμετρο και εκθέσεις από την εκστρατεία του μήνα για την ασφάλεια στον κυβερνοχώρο και από τις πανευρωπαϊκές ασκήσεις).

2.2. Σύστημα διαχείρισης και ελέγχου

2.2.1. Κίνδυνος(-οι) που έχει(-ουν) εντοπιστεί

Οι κίνδυνοι που εντοπίστηκαν είναι περιορισμένοι: υπάρχει ήδη ένας οργανισμός της Ένωσης και η εντολή του θα οριοθετηθεί, ενισχύοντας τους τομείς στους οποίους είναι σαφές ότι ο

Οργανισμός παράγει προστιθέμενη αξία και προσθέτοντας εκείνους τους νέους τομείς που χρήζουν στήριξης με βάση τις νέες προτεραιότητες και μέσα πολιτικής, συγκεκριμένα την οδηγία NIS, την επανεξέταση της Στρατηγικής της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο, το επικείμενο προσχέδιο της ΕΕ για την ασφάλεια στον κυβερνοχώρο εν όψει της συνεργασίας στην αντιμετώπιση των κρίσεων στον κυβερνοχώρο, και την πιστοποίηση ασφαλείας ΤΠΕ.

Η πρόταση περιγράφει, συνεπώς, αναλυτικά τις λειτουργίες του Οργανισμού και συμβάλλει στη βελτίωση της αποτελεσματικότητας. Η αύξηση των επιχειρησιακών αρμοδιοτήτων και των καθηκόντων δεν συνιστά πραγματικό κίνδυνο καθώς πρόκειται να λειτουργούν συμπληρωματικά στο έργο των κρατών μελών παρέχοντας στήριξη στα κράτη μέλη μετά από σχετικό αίτημα και σε σχέση με περιορισμένες και προκαθορισμένες υπηρεσίες.

Επιπλέον, το προτεινόμενο μοντέλο του οργανισμού, σύμφωνα με την κοινή προσέγγιση, διασφαλίζει ότι υπάρχει επαρκής έλεγχος ώστε ο ENISA να λειτουργεί με γνώμονα την εκπλήρωση των στόχων του. Οι επιχειρησιακοί και χρηματοοικονομικοί κίνδυνοι των προτεινόμενων αλλαγών φαίνεται ότι είναι περιορισμένοι.

Την ίδια στιγμή, είναι ανάγκη να διατεθούν επαρκείς οικονομικοί πόροι προκειμένου να διασφαλιστεί ότι ο ENISA θα μπορεί να εκτελεί τα καθήκοντα που του ανατίθενται στο πλαίσιο της νέας εντολής, συμπεριλαμβανομένου του τομέα της πιστοποίησης.

2.2.2. Προβλεπόμενη(-ες) μέθοδος(-οι) ελέγχου

Οι λογαριασμοί του οργανισμού θα υποβάλλονται προς έγκριση στο Ελεγκτικό Συνέδριο και θα υπόκεινται στη διαδικασία απαλλαγής και προβλέπονται έλεγχοι.

Επίσης, οι δραστηριότητες του οργανισμού υπόκεινται στην εποπτεία του διαμεσολαβητή, σύμφωνα με τις διατάξεις του άρθρου 228 της Συνθήκης.

Βλέπε σημείο 2.1 και σημείο 2.2.1 ανωτέρω.

2.3. Μέτρα για την πρόληψη περιπτώσεων απάτης και παρατυπίας

Να προσδιοριστούν τα ισχύοντα ή τα προβλεπόμενα μέτρα πρόληψης και προστασίας

Θα ισχύουν τα μέτρα πρόληψης και προστασίας του ENISA, ειδικότερα:

- Πριν καταβληθούν οι πληρωμές για κάθε αιτούμενη υπηρεσία ή μελέτη ελέγχονται από το προσωπικό του οργανισμού, λαμβάνοντας υπόψη τυχόν συμβατικές υποχρεώσεις, οικονομικές αρχές και ορθές δημοσιονομικές και διαχειριστικές πρακτικές. Οι διατάξεις περί καταπολέμησης της απάτης (εποπτεία, απαιτήσεις υποβολής εκθέσεων κ.λπ.) περιλαμβάνονται σε όλες τις συμφωνίες και τις συμβάσεις που συνάπτει ο οργανισμός με τους δικαιούχους των πληρωμών.

- Για την καταπολέμηση της απάτης, της διαφθοράς και άλλων παράνομων πράξεων, εφαρμόζονται, χωρίς κανέναν περιορισμό, οι διατάξεις του κανονισμού (ΕΕ, Ευρατόμ) αριθ. 883/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Σεπτεμβρίου 2013, σχετικά με τις έρευνες που πραγματοποιούνται από την Ευρωπαϊκή Υπηρεσία Καταπολέμησης της Απάτης (OLAF).

- Ο οργανισμός προσχωρεί, εντός έξι μηνών από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού, στη διοργανική συμφωνία της 25ης Μαΐου 1999 μεταξύ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της Ευρωπαϊκής Ένωσης και της Επιτροπής

των Ευρωπαϊκών Κοινοτήτων σχετικά με τις εσωτερικές έρευνες που πραγματοποιούνται από την Ευρωπαϊκή Υπηρεσία Καταπολέμησης της Απάτης (OLAF) και εκδίδει αμελλητί τις κατάλληλες διατάξεις που θα ισχύουν για όλους τους εργαζόμενους του οργανισμού.

3. ΕΚΤΙΜΩΜΕΝΕΣ ΔΗΜΟΣΙΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

3.1. Τομέας(είς) του πολυετούς δημοσιονομικού πλαισίου και γραμμή(ές) δαπανών του προϋπολογισμού που επηρεάζονται

- Υφιστάμενες γραμμές του προϋπολογισμού

Σύμφωνα με τη σειρά των τομέων του πολυετούς δημοσιονομικού πλαισίου και των γραμμών του προϋπολογισμού.

Τομέας του πολυετούς δημοσιονομικού πλαισίου	Γραμμή προϋπολογισμού	Είδος της δαπάνης	Συμμετοχή			
		ΔΠ/ΜΔΠ[52].	χωρών ΕΖΕΣ[53]	υποψηφίων για ένταξη χωρών[54]	τρίτων χωρών	κατά την έννοια του άρθρου 21 παράγραφος 2 στοιχείο β) του δημοσιονομικού κανονισμού
1α Ανταγωνιστικότητα για την ανάπτυξη και την απασχόληση	09.0203 ENISA και πιστοποίηση της ασφάλειας στον κυβερνοχώρο στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών	ΔΠ	ΝΑΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ
5 Διοικητικές δαπάνες]	09.0101 Δαπάνες σχετικές με το προσωπικό εν ενεργεία του τομέα πολιτικής Επικοινωνιακά δίκτυα, περιεχόμενο και τεχνολογίες 09.0102 Δαπάνες σχετικές με το εξωτερικό	ΜΔΠ	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ

52 ΔΠ = Διαχωριζόμενες πιστώσεις/ΜΔΠ = Μη διαχωριζόμενες πιστώσεις

53 ΕΖΕΣ: Ευρωπαϊκή Ζώνη Ελεύθερων Συναλλαγών.

54 Υποψήφιες χώρες και, εφόσον ισχύει, δυνάμει υποψήφιες για ένταξη χώρες των Δυτικών Βαλκανίων.

	προσωπικό εν ενεργεία του τομέα πολιτικής Επικοινωνιακά δίκτυα, περιεχόμενο και τεχνολογίες 09.010211 Άλλες δαπάνες διαχείρισης					

3.2. Εκτιμώμενες επιπτώσεις στις δαπάνες

3.2.1. Συνοπτική παρουσίαση των εκτιμώμενων επιπτώσεων στις δαπάνες

Σε εκατ. EUR (με 3 δεκαδικά ψηφία)

Τομέας του πολυετούς δημοσιονομικού πλαισίου:	1α	Ανταγωνιστικότητα για την ανάπτυξη και την απασχόληση

ENISA			**Βάση** **2017** **(31/12/2016)**		**2019** ***(από 01.07.2019)***	**2020**	**2021**	**2022**	**ΣΥΝΟΛΟ**
Τίτλος 1: Δαπάνες προσωπικού *(συμπεριλαμβανομένων των δαπανών που σχετίζονται με την πρόσληψη, την εκπαίδευση, τις κοινωνικοοικονομικές υποδομές και τις εξωτερικές υπηρεσίες που αφορούν το προσωπικό)*	Αναλήψεις υποχρεώσεων	(1)	6,387		9,899	12,082	13,349	13,894	**49,224**
	Πληρωμές	(2)	6,387		9,899	12,082	13,349	13,894	**49,224**
Τίτλος 2: Δαπάνες υποδομών και λειτουργίας	Αναλήψεις υποχρεώσεων	(1α)	1,770		1,957	2,232	2,461	2,565	**9,215**
	Πληρωμές	(2α)	1,770		1,957	2,232	2,461	2,565	**9,215**
Τίτλος 3: Επιχειρησιακές δαπάνες	Αναλήψεις υποχρεώσεων	(3α)	3,086		4,694	6,332	6,438	6,564	**24,028**
	Πληρωμές	(3β)	3,086		4,694	6,332	6,438	6,564	**24,028**
ΣΥΝΟΛΟ πιστώσεων	Αναλήψεις υποχρεώσεων	=1+1 α +3α	**11,244**		16,550	20,646	22,248	23,023	**82,467**

για τον ENISA	Πληρωμές	=2+2 α +3β	**11,244**		**16,550**	**20,646**	**22,248**	**23,023**	**82,467**

Τομέας του πολυετούς δημοσιονομικού πλαισίου:	**5**	«Διοικητικές δαπάνες»

Σε εκατ. EUR (με 3 δεκαδικά ψηφία)

		2019 *(από 01.07.2019)*	**2020**	**2021**	**2022**	**ΣΥΝΟΛΟ**
ΓΔ: CNECT						
• Ανθρώπινοι πόροι		0,216	0,846	0,846	0,846	**2,754**
• Άλλες διοικητικές δαπάνες		0,102	0,235	0,238	0,242	**0,817**
ΣΥΝΟΛΟ ΓΔ CNECT	Πιστώσεις	0,318	1,081	1,084	1,088	**3,571**

Οι δαπάνες προσωπικού υπολογίστηκαν σύμφωνα με την προγραμματισμένη ημερομηνία πρόσληψης (η απασχόληση προβλέπεται να αρχίσει την 01.07.2019).

Η πρόβλεψη των πόρων μετά το 2020 είναι ενδεικτική και δεν επηρεάζει τις προτάσεις της Επιτροπής για το πολυετές δημοσιονομικό πλαίσιο μετά το 2020

ΣΥΝΟΛΟ πιστώσεων για τον ΤΟΜΕΑ 5 του πολυετούς δημοσιονομικού πλαισίου	(Σύνολο πιστώσεων ανάληψης υποχρεώσεων = Σύνολο πληρωμών)	0,318	1,081	1,084	1,088	**3,571**

Σε εκατ. EUR (με 3 δεκαδικά ψηφία)

		2019	**2020**	**2021**	**2022**	**ΣΥΝΟΛΟ**
ΣΥΝΟΛΟ πιστώσεων των ΤΟΜΕΩΝ 1 έως 5 του πολυετούς δημοσιονομικού	Αναλήψεις υποχρεώσεων	16,868	21,727	23,332	24,11	**86,038**
	Πληρωμές	16,868	21,727	23,332	24,11	**86,038**

πλαισίου						

3.2.2. Εκτιμώμενες επιπτώσεις στις πιστώσεις του Οργανισμού

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

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

Πιστώσεις ανάληψης υποχρεώσεων σε εκατ. EUR (με 3 δεκαδικά ψηφία)

Να προσδιοριστούν οι στόχοι και τα αποτελέσματα[55] ⇩	**2019**	**2020**	**2021**	**2022**	**ΣΥΝΟΛΟ**
Αύξηση των ικανοτήτων και της ετοιμότητας των κρατών μελών και των επιχειρήσεων	1,408	1,900	1,931	1,969	7,208
Βελτίωση της συνεργασίας και του συντονισμού στα κράτη μέλη και τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ.	0,939	1,266	1,288	1,313	4,806
Αύξηση των ικανοτήτων σε επίπεδο ΕΕ για τη συμπλήρωση της δράσης των κρατών μελών, ιδίως στην περίπτωση των διασυνοριακών κρίσεων στον κυβερνοχώρο.	0,704	0,950	0,965	0,985	3,604
Αυξημένη ευαισθητοποίηση των πολιτών και των επιχειρήσεων σε ζητήματα ασφάλειας στον κυβερνοχώρο.	0,704	0,950	0,965	0,985	3,604
Ενίσχυση της εμπιστοσύνης στην ψηφιακή ενιαία αγορά και την ψηφιακή καινοτομία μέσα από την αύξηση της συνολικής διαφάνειας της διασφάλισης της ασφάλειας στον κυβερνοχώρο των προϊόντων και υπηρεσιών ΤΠΕ.	0,939	1,266	1,288	1,313	4,806
ΣΥΝΟΛΙΚΟ ΚΟΣΤΟΣ	4,694	6,332	6,437	6,565	24,028

[55] Ο παρών πίνακας παρουσιάζει μόνο τις επιχειρησιακές δαπάνες για τον τίτλο 3.

3.2.3. Εκτιμώμενες επιπτώσεις στους ανθρώπινους πόρους του Οργανισμού

3.2.3.1. Συνοπτική παρουσίαση

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

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

Σε εκατ. EUR (με 3 δεκαδικά ψηφία)

	Τ3/4 2019	**2020**	**2021**	**2022**
Έκτακτοι υπάλληλοι (Βαθμοί AD)	4,242	5,695	6,381	6,709
Έκτακτοι υπάλληλοι (Βαθμοί AST)	1,601	1,998	2,217	2,217
Συμβασιούχοι υπάλληλοι	2,041	2,041	2,041	2,041
Αποσπασμένοι εθνικοί εμπειρογνώμονες	0,306	0,447	0,656	0,796
ΣΥΝΟΛΟ	**8,190**	**10,181**	**11,295**	**11,763**

Οι δαπάνες προσωπικού υπολογίστηκαν σύμφωνα με την προγραμματισμένη ημερομηνία πρόσληψης (για το υφιστάμενο προσωπικό του ENISA θεωρήθηκε ότι η πλήρης απασχόληση θα αρχίσει από την 01.01.2019). Για τους νέους υπαλλήλους προβλέφθηκε σταδιακή έναρξη της απασχόλησης από τις 01.07.2019 και πλήρης απασχόληση από το 2022. Η πρόβλεψη των πόρων μετά το 2020 είναι ενδεικτική και δεν επηρεάζει τις προτάσεις της Επιτροπής για το πολυετές δημοσιονομικό πλαίσιο μετά το 2020.

Εκτιμώμενες επιπτώσεις στο προσωπικό (επιπλέον ΙΠΑ) – πίνακας προσωπικού

Ομάδα καθηκόντων και βαθμός	2017 **Υφιστάμενος ENISA**	Τ3/4 2019	2020	2021	2022
AD16					
AD15	1				
AD14					
AD13					
AD12	3	3			
AD11					
AD10	5				
AD9	10	2			
AD8	15	4	2		1
AD7			3	3	2
AD6			3	3	
AD5					
Σύνολο AD	34	9	8	6	3
AST11					
AST10					
AST9					
AST8					

AST7 AST6 AST5 AST4 AST3 AST2 AST1	2 5 5 2	1 2	1 1	1	
Σύνολο AST	14	3	2	1	
AST/SC 6 AST/SC 5 AST/SC 4 AST/SC 3 AST/SC 2 AST/SC 1					
Σύνολο AST/SC					
ΓΕΝΙΚΟ ΣΥΝΟΛΟ	48	12	10	7	3

Τα καθήκοντα των επιπλέον υπαλλήλων βαθμού AD/AST για την επίτευξη των στόχων του μέσου όπως περιγράφονται στην ενότητα 1.4.2:

Καθήκοντα	AD	AST	AEE	Σύνολο
Χάραξη πολιτικής και ανάπτυξη ικανοτήτων	8	1		9
Επιχειρησιακή συνεργασία	8	1	7	16
Πιστοποίηση (καθήκοντα σχετικά με την αγορά)	9	3	2	14
Γνώσεις, πληροφόρηση και ευαισθητοποίηση	1	1		2
ΣΥΝΟΛΟ	26	6	9	41

Περιγραφή των προς εκτέλεση καθηκόντων:

Καθήκοντα	**Πρόσθετοι απαιτούμενοι πόροι**
Χάραξη και εφαρμογή πολιτικής της ΕΕ & ανάπτυξη ικανοτήτων	Στα καθήκοντα περιλαμβάνονται: συνδρομή της ομάδας συνεργασίας, υποστήριξη της συνεπούς εφαρμογής της NIS σε διασυνοριακή κλίμακα, τακτική υποβολή εκθέσεων σχετικά με την κατάσταση εφαρμογής του νομικού πλαισίου της ΕΕ· παροχή συμβουλών και συντονισμός τομεακών πρωτοβουλιών για την ασφάλεια στον κυβερνοχώρο, μεταξύ άλλων στους τομείς της ενέργειας, των μεταφορών (π.χ. αεροπορικά/οδικά/θαλάσσια συνδεδεμένα οχήματα), της υγείας, των οικονομικών, παροχή στήριξης στη δημιουργία κέντρων κοινοχρησίας και ανάλυσης πληροφοριών (ISAC) σε διάφορους τομείς.
Επιχειρησιακή συνεργασία και διαχείριση κρίσεων	**Στα καθήκοντα περιλαμβάνονται:** παροχή γραμματειακής υποστήριξης στο δίκτυο CSIRT

	διασφαλίζοντας μεταξύ άλλων την εύρυθμη λειτουργία της υποδομής ΤΠ και των διαύλων επικοινωνίας του δικτύου CSIRT. Επίτευξη δομημένης συνεργασίας με τη CERT-EU, το EC3 και άλλους σχετικούς φορείς της ΕΕ. Διοργάνωση των **ασκήσεων Cyber Europe**[56] - καθήκοντα που σχετίζονται με την πιο συχνή πραγματοποίηση της άσκησης, σε ετήσια βάση και όχι ανά διετία, και μέριμνα ώστε οι ασκήσεις να εξετάζουν το συμβάν σε όλη την εξέλιξή του. **Τεχνική βοήθεια** - στα καθήκοντα περιλαμβάνονται: δομημένη συνεργασία με την CERT-EU για την παροχή τεχνικής βοήθειας σε περίπτωση σημαντικών συμβάντων και για την υποστήριξη της ανάλυσης των συμβάντων. Εδώ εντάσσεται η παροχή συνδρομής στα κράτη μέλη για την αντιμετώπιση των συμβάντων και την ανάλυση των τρωτών σημείων, των σφαλμάτων και των συμβάντων. Διευκόλυνση της συνεργασίας μεταξύ μεμονωμένων κρατών μελών για την αντιμετώπιση έκτακτων αναγκών μέσω της ανάλυσης και της συγκέντρωσης εθνικών εκθέσεων κατάστασης που βασίζονται στις πληροφορίες που διατίθενται στον Οργανισμό από τα κράτη μέλη και άλλες οντότητες. **Προσχέδιο για συντονισμένη αντιμετώπιση των μεγάλης κλίμακας διασυνοριακών συμβάντων** - ο Οργανισμός θα συμβάλλει στην ανάπτυξη κοινής αντιμετώπισης, σε επίπεδο Ένωσης και κρατών μελών, των μεγάλης κλίμακας διασυνοριακών συμβάντων ή κρίσεων που αφορούν την ασφάλεια στον κυβερνοχώρο μέσω μιας σειράς καθηκόντων, από τη συμβολή στην διαμόρφωση εικόνας για την κατάσταση σε επίπεδο ΕΕ έως τη δοκιμή των σχεδίων συνεργασίας σε περίπτωση συμβάντος. **Εκ των υστέρων τεχνικές έρευνες σχετικά με συμβάντα** - διενέργεια ή συμβολή στη διενέργεια εκ των υστέρων τεχνικών ερευνών σχετικά με συμβάντα σε συνεργασία με το δίκτυο CSIRT, με σκοπό την έκδοση συστάσεων και την ενίσχυση των ικανοτήτων μέσω δημόσιων εκθέσεων για την καλύτερη πρόληψη μελλοντικών συμβάντων.
Καθήκοντα σχετικά με την	Στα καθήκοντα περιλαμβάνεται η ενεργή υποστήριξη του

[56] Η Cyber Europe είναι η μεγαλύτερη και πιο ολοκληρωμένη έως σήμερα άσκηση της ΕΕ για την ασφάλεια στον κυβερνοχώρο με συμμετοχή περισσότερων από 700 επαγγελματιών στον τομέα της ασφάλειας στον κυβερνοχώρο από το σύνολο των 28 κρατών μελών. Πραγματοποιείται ανά διετία. Στην αξιολόγηση του ENISA και στη στρατηγική της ΕΕ για την ασφάλεια στον κυβερνοχώρο του 2013 επισημαίνεται ότι πολλοί άμεσα ενδιαφερόμενοι συνιστούν την διοργάνωση του Cyber Europe σε ετήσια βάση, δεδομένης της ταχέως εξελισσόμενης φύσης των απειλών στον κυβερνοχώρο. Αυτό, ωστόσο, δεν είναι προς το παρόν εφικτό λόγω των περιορισμένων πόρων που έχει στη διάθεσή του ο Οργανισμός.

αγορά (τυποποίηση, πιστοποίηση)	έργου που επιτελείται βάσει του πλαισίου πιστοποίησης, συμπεριλαμβανομένης της παροχής τεχνικής εμπειρογνωσίας για την επεξεργασία υποψήφιων ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο. Στα καθήκοντα περιλαμβάνεται επίσης η παροχή υποστήριξης στη χάραξη και εφαρμογή της ενωσιακής πολιτικής σχετικά με την τυποποίηση, την πιστοποίηση και το παρατηρητήριο αγοράς – αυτό προϋποθέτει διευκόλυνση της αξιοποίησης των προτύπων διαχείρισης κινδύνων για τα ηλεκτρονικά προϊόντα, δίκτυα και υπηρεσίες και παροχή συμβουλών στους φορείς εκμετάλλευσης βασικών υπηρεσιών και τους παρόχους ψηφιακών υπηρεσιών σχετικά με τις απαιτήσεις τεχνικής ασφάλειας. Τέλος, στα καθήκοντα περιλαμβάνεται η ανάλυση των βασικών τάσεων στην αγορά της ασφάλειας στον κυβερνοχώρο.
Γνώση και πληροφορίες, ευαισθητοποίηση:	Με στόχο τη διευκόλυνση της πρόσβασης σε καλύτερα δομημένες πληροφορίες σχετικά με τους κινδύνους για την ασφάλεια στον κυβερνοχώρο και τα πιθανά διορθωτικά μέτρα, η πρόταση αναθέτει στον Οργανισμό το νέο καθήκον της ανάπτυξης και διατήρησης του «κόμβου ανταλλαγής πληροφοριών» της Ένωσης. Στα καθήκοντα περιλαμβάνεται η συγκέντρωση, οργάνωση και διάθεση στο κοινό, μέσω ειδικής δικτυακής πύλης, πληροφοριών σχετικά με την ασφάλεια των συστημάτων δικτύου ή πληροφοριών, ιδίως δε την ασφάλεια στον κυβερνοχώρο, τις οποίες παρέχουν τα θεσμικά όργανα, οι οργανισμοί και οι φορείς της ΕΕ. Στα καθήκοντα περιλαμβάνεται επίσης η υποστήριξη των δραστηριοτήτων του ENISA στον τομέα της ευαισθητοποίησης με στόχο να δοθεί στον οργανισμό η δυνατότητα να κλιμακώσει την προσπάθειά του.

Εκτιμώμενες ανάγκες της αρμόδιας ΓΔ σε ανθρώπινους πόρους

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

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

Εκτίμηση η οποία πρέπει να διατυπωθεί σε ακέραιο αριθμό (ή το πολύ με ένα δεκαδικό ψηφίο)

		Πρόσθετο προσωπικό			
	Βάση αναφοράς 2017	Τ3/4 2019	2020	2021	2020
• **Θέσεις απασχόλησης του πίνακα προσωπικού (θέσεις μόνιμων και έκτακτων**					

υπαλλήλων)					
09 01 01 01 (έδρα και γραφεία αντιπροσωπείας της Επιτροπής)	1	2	3		
• **Εξωτερικό προσωπικό (σε μονάδα ισοδυνάμου πλήρους απασχόλησης: ΙΠΑ)**[57]					
09 01 02 01 (AC, END, INT από το συνολικό κονδύλιο)	1	2			
ΣΥΝΟΛΟ		**4**	**3**		

Περιγραφή των προς εκτέλεση καθηκόντων:

Μόνιμοι και έκτακτοι υπάλληλοι	Εκπροσώπηση της Επιτροπής στο διοικητικό συμβούλιο του οργανισμού. Σύνταξη της γνώμης της Επιτροπής σχετικά με το ενιαίο έγγραφο προγραμματισμού του ENISA και την παρακολούθηση της υλοποίησής του. Επίβλεψη της κατάρτισης του προϋπολογισμού του οργανισμού και παρακολούθηση της εκτέλεσης του προϋπολογισμού. Παροχή συνδρομής στον οργανισμό για την ανάπτυξη των δραστηριοτήτων του σύμφωνα με τις πολιτικές της Ένωσης, μεταξύ άλλων μέσω συμμετοχής σε σχετικές συνεδριάσεις. Επίβλεψη της εφαρμογής του πλαισίου για τα ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο των προϊόντων και υπηρεσιών ΤΠΕ. Διατήρηση σταθερής επαφής με τα κράτη μέλη και τους άλλους συναφείς άμεσα ενδιαφερόμενους σε σχέση με τις προσπάθειες πιστοποίησης. Συνεργασία με τον ENISA σε σχέση με τα υποψήφια συστήματα. Επεξεργασία υποψήφιων ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο.
Εξωτερικό προσωπικό	Όπως ανωτέρω

3.2.4. Συμβατότητα με το ισχύον πολυετές δημοσιονομικό πλαίσιο

– ☐ Η πρόταση/πρωτοβουλία είναι συμβατή με τον ισχύον πολυετές δημοσιονομικό πλαίσιο.

– ☒ Η πρόταση/πρωτοβουλία απαιτεί αναπρογραμματισμό του σχετικού τομέα του πολυετούς δημοσιονομικού πλαισίου.

[57] AC = Συμβασιούχος υπάλληλος· AL = Τοπικός υπάλληλος· END = Αποσπασμένος εθνικός εμπειρογνώμονας· INT = Προσωρινό προσωπικό οργανισμού· JED = Νεαρός εμπειρογνώμονας σε αντιπροσωπεία.

Η πρόταση προϋποθέτει αναπρογραμματισμό του άρθρου 09 02 03 λόγω της αναθεώρησης της εντολής του ENISA, η οποία αναθέτει στον οργανισμό νέα καθήκοντα που σχετίζονται, μεταξύ άλλων, με την εφαρμογή της οδηγίας NIS και με το ευρωπαϊκό πλαίσιο πιστοποίησης της ασφάλειας στον κυβερνοχώρο. Τα αντίστοιχα ποσά:

Έτος	Προβλεπόμενο	Αιτούμενο
2019	10,739	16,550
2020	10,954	20,646
2021	Άνευ αντικειμένου	22,248*
2022	Άνευ αντικειμένου	23,023*

* Πρόκειται για εκτίμηση. Η χρηματοδότηση της ΕΕ μετά το 2020 θα εξετασθεί στο πλαίσιο διαλόγου στον οποίο θα συμμετάσχουν όλες οι υπηρεσίες της Επιτροπής επί του συνόλου των προτάσεων για την περίοδο μετά το 2020. Αυτό σημαίνει ότι μετά την υποβολή από την Επιτροπή της πρότασής της για το επόμενο πολυετές δημοσιονομικό πλαίσιο, η Επιτροπή θα υποβάλει τροποποιημένο νομοθετικό δημοσιονομικό δελτίο, λαμβάνοντας υπόψη τα συμπεράσματα της εκτίμησης επιπτώσεων[58].

– ☐ Η πρόταση/πρωτοβουλία απαιτεί τη χρησιμοποίηση του μέσου ευελιξίας ή την αναθεώρηση του πολυετούς δημοσιονομικού πλαισίου[59].

3.2.5. Συμμετοχή τρίτων μερών στη χρηματοδότηση

– ☐ Η πρόταση/πρωτοβουλία δεν προβλέπει συγχρηματοδότηση από τρίτα μέρη.

– ☒ Η πρόταση/πρωτοβουλία προβλέπει τη συγχρηματοδότηση που εκτιμάται παρακάτω:

	Έτος **2019**	Έτος **2020**	Έτος **2021**	Έτος **2022**
ΕΖΕΣ	p.m[60].	p.m.	p.m.	p.m.

3.3. Εκτιμώμενες επιπτώσεις στα έσοδα

– ☒ Η πρόταση/πρωτοβουλία δεν έχει δημοσιονομικές επιπτώσεις στα έσοδα.

58 Σύνδεσμος με τη σελίδα για την εκτίμηση επιπτώσεων

59 Βλ. άρθρα 11 και 17 του κανονισμού (ΕΕ, Ευρατόμ) αριθ. 1311/2013 του Συμβουλίου για τον καθορισμό του πολυετούς δημοσιονομικού πλαισίου για την περίοδο 2014-2020.

60 Το ακριβές ποσό για τα επόμενη έτη θα γίνει γνωστό μετά τον καθορισμό του συντελεστή αναλογικότητας του ΕΖΕΣ για το αντίστοιχο έτος.

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

  – ☐ στους ιδίους πόρους

  – ☐ στα διάφορα έσοδα