Συμβούλιο
της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 29 Μαΐου 2018
(OR. en)

9350/18

Διοργανικός φάκελος:
2017/0225 (COD)

CYBER 115
TELECOM 152
CODEC 860
COPEN 163
COPS 175
COSI 129
CSC 170
CSCI 80
IND 143
JAI 514
JAIEX 55
POLMIL 61
RELEX 463

ΣΗΜΕΙΩΜΑ

Αποστολέας:	Προεδρία
Αποδέκτης:	Συμβούλιο
αριθ. προηγ. εγγρ.:	8834/18
Αριθ. εγγρ. Επιτρ.:	12183/17
Θέμα:	Πρόταση ΚΑΝΟΝΙΣΜΟΥ 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») - Γενική προσέγγιση

I. ΕΙΣΑΓΩΓΗ

1. Στις 13 Σεπτεμβρίου 2017, στο πλαίσιο της στρατηγικής για την ψηφιακή ενιαία αγορά, η Επιτροπή ενέκρινε και διαβίβασε στο Συμβούλιο και στο Ευρωπαϊκό Κοινοβούλιο την ως άνω πρόταση[1] με νομική βάση το άρθρο 114 της ΣΛΕΕ. Ως μέρος της λεγόμενης «δέσμης μέτρων για την ασφάλεια στον κυβερνοχώρο», η πρόταση αυτή στοχεύει στην επίτευξη υψηλού επιπέδου ασφάλειας στον κυβερνοχώρο, την ανθεκτικότητα του κυβερνοχώρου και την εμπιστοσύνη εντός της Ένωσης, με σκοπό τη διασφάλιση της ορθής λειτουργίας της εσωτερικής αγοράς.

2. Ο προτεινόμενος κανονισμός καθορίζει τους στόχους, τα καθήκοντα και τις οργανωτικές πτυχές του ENISA (του Οργανισμού της ΕΕ για την ασφάλεια στον κυβερνοχώρο) και δημιουργεί ένα πλαίσιο για τη δημιουργία ευρωπαϊκών συστημάτων πιστοποίησης στον τομέα της ασφάλειας στον κυβερνοχώρο με σκοπό την εξασφάλιση επαρκούς επιπέδου ασφάλειας στον κυβερνοχώρο για προϊόντα και υπηρεσίες ΤΠΕ στην Ένωση. Η πρόταση της Επιτροπής συνοδεύεται από εκτίμηση επιπτώσεων, η οποία εξετάζει ένα συγκεκριμένο σύνολο οκτώ επιλογών πολιτικής, οι οποίες καλύπτουν την επανεξέταση του ENISA και την πιστοποίηση της ασφάλειας στον κυβερνοχώρο στον τομέα των ΤΠΕ.

3. Ο προτεινόμενος κανονισμός περιλαμβάνει δύο βασικές συνιστώσες:

   - μόνιμη εντολή προς τον Οργανισμό με οριοθετημένο πεδίο εφαρμογής ενόψει των αναγκών στο πλαίσιο των νέων πολιτικών προτεραιοτήτων και μέσων, και ανανεωμένη δέσμη αρμοδιοτήτων και καθηκόντων για τον Οργανισμό ώστε να καταστεί δυνατή η αποτελεσματική και αποδοτική στήριξη στα κράτη μέλη, τα θεσμικά όργανα της ΕΕ και τους άλλους φορείς στις προσπάθειές τους για την εξασφάλιση ενός ασφαλούς κυβερνοχώρου·

   - ευρωπαϊκό πλαίσιο πιστοποίησης της ασφάλειας στον κυβερνοχώρο για προϊόντα και υπηρεσίες ΤΠΕ, καθώς και κανόνες για τα ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο που να επιτρέπουν στα πιστοποιητικά που εκδίδονται στο πλαίσιο των εν λόγω συστημάτων να είναι έγκυρα και να αναγνωρίζονται σε όλα τα κράτη μέλη και να αντιμετωπίζουν τον τρέχοντα κατακερματισμό της αγοράς.

[1] Έγγρ. 12183/17, 12183/1/17 REV 1, 12183/2/17 REV 2.

4. Τον Οκτώβριο του 2017, το Ευρωπαϊκό Συμβούλιο[2] ζήτησε οι προτάσεις της Επιτροπής για την ασφάλεια στον κυβερνοχώρο να αναπτυχθούν κατά τρόπο ολιστικό, να παραδοθούν εγκαίρως και να εξεταστούν χωρίς καθυστέρηση, βάσει σχεδίου δράσης που θα καταρτιστεί από το Συμβούλιο.

5. Στις 12 Δεκεμβρίου 2017, το Συμβούλιο Γενικών Υποθέσεων ενέκρινε σχέδιο δράσης[3] για την εφαρμογή των συμπερασμάτων του Συμβουλίου[4] για την κοινή ανακοίνωση[5] προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: «Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ». Το σχέδιο δράσης αποτυπώνει τη φιλοδοξία του Συμβουλίου να επιτευχθεί γενική προσέγγιση σχετικά με την πρόταση έως τα τέλη Ιουνίου 2018.

6. Στο Ευρωπαϊκό Κοινοβούλιο, η κ. Angelika NIEBLER (ITRE, ΕΛΚ) ορίστηκε ως εισηγήτρια. Η επιτροπή ITRE αναμένεται να ψηφίσει την έκθεσή της στις 19 Ιουνίου 2018.

7. Η Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή γνωμοδότησε στις 14 Φεβρουαρίου 2018.

II. ΕΡΓΑΣΙΕΣ ΣΤΟ ΠΛΑΙΣΙΟ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

8. Η Επιτροπή υπέβαλε την πρόταση και τη σχετική εκτίμηση των επιπτώσεων στην οριζόντια Ομάδα εργασίας για θέματα κυβερνοχώρου (εφεξής: Ομάδα) στις 26 Σεπτεμβρίου 2017, και ακολούθησε εξέταση της εκτίμησης των επιπτώσεων από την Ομάδα στις 20 Οκτωβρίου 2017. Οι συζητήσεις επικεντρώθηκαν κατόπιν στην επιχειρησιακή ικανότητα του Οργανισμού και το πεδίο της αλληλεπίδρασης με τις εθνικές αρμόδιες αρχές, καθώς και στον αντίκτυπο του πλαισίου πιστοποίησης στην αγορά και την ανταγωνιστικότητα των επιχειρήσεων. Σε γενικές γραμμές, οι αντιπροσωπίες υποδέχτηκαν θετικά τόσο την εκτίμηση επιπτώσεων όσο και την πρόταση.

---

2 EUCO 14/17, παράγραφος 11.
3 Έγγρ. 15748/17.
4 Έγγρ. 14435/17.
5 Έγγρ. 12211/17.

9. Η συζήτηση της πρότασης αυτής από την Ομάδα ξεκίνησε τον Νοέμβριο του 2017 κατά την εσθονική Προεδρία και συνέχισε υπό τη βουλγαρική Προεδρία. Πραγματοποιήθηκαν 12 συνεδριάσεις για την πρόταση, οι οποίες κατέληξαν σε οκτώ διαδοχικές αναθεωρημένες εκδοχές της πρότασης με σκοπό την επίτευξη συμφωνίας για γενική προσέγγιση στο προσεχές Συμβούλιο ΤΤΕ (Τηλεπικοινωνίες) που θα πραγματοποιηθεί στις 8 Ιουνίου 2018.

10. Τα αποτελέσματα των συζητήσεων της Ομάδας στις 14 και 15 Μαΐου 2018 καθώς και το αναθεωρημένο συμβιβαστικό κείμενο της Προεδρίας παρατίθενται στο παράρτημα του παρόντος σημειώματος. Οι αιτιολογικές σκέψεις τροποποιήθηκαν ώστε να λαμβάνουν υπόψη τις αλλαγές στο διατακτικό. Όλες οι τροποποιήσεις επί των αρχικών προτάσεων της Επιτροπής εμφανίζονται με **έντονα στοιχεία** ή [...]. Οι αλλαγές σε σχέση με το πλέον πρόσφατο έγγραφο της Ομάδας (8834/18) σημειώνονται με **έντονα υπογραμμισμένα στοιχεία** και όλες οι διαγραφές με **[...]**.

III. ΣΥΜΠΕΡΑΣΜΑ

11. Το συμβιβαστικό κείμενο της Προεδρίας, ως έχει στο παράρτημα, αντικατοπτρίζει τις προσπάθειες της Προεδρίας και των κρατών μελών να επιτύχουν την κατάλληλη ισορροπία στο κείμενο.

12. Στις 25 Μαΐου 2018, η Επιτροπή των Μόνιμων Αντιπροσώπων κατέληξε σε συμφωνία επί του συμβιβαστικού κειμένου της Προεδρίας, με τροπολογίες στα άρθρα 19 παράγραφος 5 και 48 παράγραφος 5, όπως παρατίθεται στο παράρτημα.

13. Το Συμβούλιο καλείται συνεπώς να εγκρίνει γενική προσέγγιση κατά τη σύνοδό του στις 8 Ιουνίου 2018 και να αναθέσει στην Προεδρία να ξεκινήσει διαπραγματεύσεις με τους εκπροσώπους του Ευρωπαϊκού Κοινοβουλίου και της Ευρωπαϊκής Επιτροπής σχετικά με το θέμα αυτό.

ΠΑΡΑΡΤΗΜΑ

Πρόταση

ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

σχετικά με τον ENISA, τον *«Οργανισμό της [...] Ευρωπαϊκής Ένωσης 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,

Μετά τη διαβίβαση του σχεδίου νομοθετικής πράξης στα εθνικά κοινοβούλια,

Έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής[6],

Έχοντας υπόψη τη γνώμη της Επιτροπής των Περιφερειών[7],

Αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία,

---

[6] ΕΕ C της , σ. .

[7] ΕΕ C της , σ. .

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 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 του 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[8] 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 ενέκριναν τον κανονισμό (ΕΚ) αριθ. 1007/2008[9] για την παράταση της θητείας του Οργανισμού έως τον Μάρτιο του 2012. Ο κανονισμός (ΕΚ) αριθ. 580/2011[10] 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[11] 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.

---

8 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).

9 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).

10 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).

11 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).

(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 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 στηρίζει** [...] τις εθνικές προσπάθειες και **να συμβάλλει προδραστικά** στις προσπάθειες σε επίπεδο Ένωσης εκτελώντας παράλληλα 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 **και τις ειδικές ανά τομέα πτυχές αυτού του πεδίου προκειμένου να ενισχύσει τη σημασία της πολιτικής και της νομοθεσίας της ΕΕ που σχετίζεται με την ασφάλεια στον κυβερνοχώρο και να επιτρέψει τη συνεπή εφαρμογή αυτών σε εθνικό επίπεδο** [...]. 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** [...] 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 [...] **απειλών** 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 ομάδων παρέμβασης για συμβάντα που αφορούν την ασφάλεια των υπολογιστών (CSIRT), με σκοπό την επίτευξη υψηλού κοινού επιπέδου ωριμότητάς τους στην Ένωση. **Οι δραστηριότητες που διεξάγει ο ENISA σχετικά με τις επιχειρησιακές δυνατότητες των κρατών μελών θα πρέπει να είναι απλώς συμπληρωματικές προς τις δράσεις που αναλαμβάνουν τα ίδια τα κράτη μέλη για να εκπληρώνουν τις υποχρεώσεις τους που απορρέουν από την οδηγία NIS (οδηγία σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση) και συνεπώς δεν θα πρέπει να τις υπερσκελίζουν** [...].

(15α) Ο Οργανισμός θα πρέπει επίσης να συμβάλλει στην ανάπτυξη και την επικαιροποίηση των στρατηγικών της Ένωσης και, κατόπιν αιτήματος, 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 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, μεταξύ άλλων όσον αφορά διασυνοριακές εξαρτήσεις σε σχέση με κινδύνους και συμβάντα.

(17) Με στόχο να δοθούν κίνητρα για τη συνεργασία δημόσιου και ιδιωτικού τομέα και εντός του ιδιωτικού τομέα, [...] **ο Οργανισμός θα πρέπει** να στηρίζει **την ανταλλαγή πληροφοριών στους τομείς και μεταξύ των τομέων, ιδίως σε αυτούς που αναφέρονται στον κατάλογο του παραρτήματος ΙΙ της οδηγίας (ΕΕ) 2016/1148, προσφέροντας βέλτιστες πρακτικές και καθοδήγηση για τα διαθέσιμα εργαλεία και τη διαδικασία, καθώς και παρέχοντας καθοδήγηση για τον τρόπο με τον οποίο θα αντιμετωπίζονται κανονιστικά ζητήματα που σχετίζονται με την ανταλλαγή πληροφοριών, για παράδειγμα μέσω της διευκόλυνσης** [...] της θέσπισης τομεακών κέντρων κοινοχρησίας και ανάλυσης πληροφοριών (ISACs) [...].

(18) Ο Οργανισμός θα πρέπει να συγκεντρώνει και να αναλύει εθνικές εκθέσεις από τις CSIRT και τη CERT-EU **οι οποίες ανταλλάσσονται σε εθελοντική βάση με σκοπό τη διευκόλυνση των κρατών μελών** για τον καθορισμό κοινών [...] **διαδικασιών**, γλώσσας και ορολογίας 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 [...] **εντός** 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. Η λειτουργία αυτή θα πρέπει **να εκτελείται σύμφωνα με την εντολή του Οργανισμού όπως αυτή καθορίζεται από τον παρόντα κανονισμό και με βάση μια προσέγγιση που θα αποφασιστεί από τα κράτη μέλη στο πλαίσιο της σύστασης της Επιτροπής για τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο. Αυτό θα μπορούσε** 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 [...] **τακτικών** ασκήσεων ασφάλειας στον κυβερνοχώρο.

(20) [...] **Για τη στήριξη** της επιχειρησιακής **συνεργασίας** [...], ο Οργανισμός θα πρέπει να χρησιμοποιεί τη διαθέσιμη **τεχνική και επιχειρησιακή** εμπειρογνωσία της CERT-EU μέσω διαρθρωμένης συνεργασίας [...]. Όπου συντρέχει περίπτωση, θα πρέπει να θεσπίζονται συγκεκριμένες ρυθμίσεις μεταξύ των δύο οργανισμών με σκοπό τον καθορισμό της πρακτικής εφαρμογής της εν λόγω συνεργασίας **και την αποφυγή αλληλοεπικάλυψης των δραστηριοτήτων**.

(21) Συμμορφούμενος προς τα καθήκοντά του [...] που αφορούν **τη στήριξη της επιχειρησιακής συνεργασίας στο πλαίσιο του δικτύου των CSIRT**, ο Οργανισμός θα πρέπει να μπορεί να παρέχει στήριξη στα κράτη μέλη **κατόπιν αιτήματός τους**, όπως για παράδειγμα παρέχοντας συμβουλές **για το πώς να βελτιώσουν τις δυνατότητές τους να προλαμβάνουν, να εντοπίζουν και να αποκρίνονται σε περιστατικά, [...] διευκολύνοντας** την [...] τεχνική **διαχείριση περιστατικών που έχουν σημαντικό ή ουσιαστικό αντίκτυπο** [...] ή **εξασφαλίζοντας** τη διενέργεια αναλύσεων απειλών και περιστατικών. **Η διευκόλυνση της τεχνικής διαχείρισης περιστατικών που έχουν σημαντικό ή ουσιαστικό αντίκτυπο θα πρέπει να περιλαμβάνει ιδίως τη στήριξη από τον ENISA της εθελοντικής ανταλλαγής τεχνικών λύσεων μεταξύ των κρατών μελών ή την παραγωγή συνδυαστικών τεχνικών πληροφοριών, όπως τεχνικών λύσεων που ανταλλάσσουν σε εθελοντική βάση τα κράτη μέλη.** 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 στο [...] καθήκον του **να στηρίζει την επιχειρησιακή συνεργασία**.

(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 **και σε στενή συνεργασία με τα κράτη μέλη** 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 [...] ή τα ενιαία κέντρα επαφής της οδηγίας NIS **(αμφότερα σε εθελοντική βάση)**, 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) **Η στήριξη από τον Οργανισμό για τις** εκ των υστέρων τεχνικές **έρευνες** [...] περιστατικών με ουσιαστικό αντίκτυπο [...] κατόπιν αιτήματος [...] των [...] **ενδιαφερόμενων** κρατών μελών θα πρέπει να επικεντρώνεται στην πρόληψη μελλοντικών περιστατικών [...]. **Τα ενδιαφερόμενα κράτη μέλη θα πρέπει να παρέχουν τις απαραίτητες πληροφορίες προκειμένου να μπορεί ο Οργανισμός να στηρίζει αποτελεσματικά την τεχνική έρευνα.**

(24) [...]

(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 **που είναι διαθέσιμες στο κοινό ή ανταλλάσσονται σε εθελοντική βάση** 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 [...] **περιστατικών** που σχετίζονται με την ασφάλεια στον κυβερνοχώρο, πραγματοποιώντας αναλύσεις των απειλών και των συμβάντων.

(27) Προκειμένου να αυξήσει την ανθεκτικότητα της Ένωσης, ο Οργανισμός θα πρέπει να αναπτύξει αριστεία στο ζήτημα της ασφάλειας **στον κυβερνοχώρο υποδομών που στηρίζουν ιδίως τους τομείς που αναφέρονται στον κατάλογο του παραρτήματος ΙΙ της οδηγίας NIS και εκείνων που χρησιμοποιούνται από τους παρόχους ψηφιακών υπηρεσιών που αναφέρονται στον κατάλογο του παραρτήματος ΙΙΙ της εν λόγω οδηγίας** [...] παρέχοντας 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 Europol, ο Ευρωπαϊκός Οργανισμός για τη λειτουργική διαχείριση συστημάτων ΤΠ μεγάλης κλίμακας (eu-LISA), ο Ευρωπαϊκός Οργανισμός Ασφάλειας της Αεροπορίας (EOAA), **ο Ευρωπαϊκός Οργανισμός του Παγκόσμιου Δορυφορικού Συστήματος Πλοήγησης (Οργανισμός του GNSS)** και κάθε άλλος οργανισμός της ΕΕ που εμπλέκεται στην ασφάλεια ΤΠ. 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, **υπό την ιδιότητά** του ως [...] Γραμματείας του δικτύου 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 τακτική 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 τους.

(36) Ο Οργανισμός θα πρέπει να χρησιμοποιεί πλήρως 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 οργανισμούς της Ένωσης και, όπου είναι σκόπιμο, τα κράτη μέλη, εφόσον το ζητήσουν, σχετικά με τις ερευνητικές ανάγκες στον τομέα της ασφάλειας [...] στον κυβερνοχώρο. **Προκειμένου να προσδιοριστούν οι ερευνητικές ανάγκες και προτεραιότητες, ο Οργανισμός θα πρέπει επίσης να συμβουλεύεται τις οικείες ομάδες χρηστών.**

(37) [...] Οι **απειλές** στον κυβερνοχώρο είναι παγκόσμιες. Υπάρχει ανάγκη στενότερης διεθνούς συνεργασίας για τη βελτίωση των προτύπων ασφαλείας **στον κυβερνοχώρο**, συμπεριλαμβανομένου 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 ευρωπαϊκή 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 οργανισμούς της Ένωσης.

(38) Ο Οργανισμός θα πρέπει να είναι ικανός να ανταποκρίνεται σε συγκεκριμένα 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 **που περιλαμβάνει την υλοποίηση του ετήσιου προγράμματος εργασίας του Οργανισμού** και να την υποβάλλει στο διοικητικό συμβούλιο, να εκπονεί σχέδιο της κατάστασης των εκτιμώμενων 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[12]. 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[13]. 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.

---

12 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).

13 ΕΕ L 8 της 12.1.2001, σ. 1.

(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 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) [...]

(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 των ευρωπαϊκών εταιρειών σε εθνικό, ευρωπαϊκό και παγκόσμιο επίπεδο. Αφετέρου, μειώνει την επιλογή βιώσιμων και χρήσιμων τεχνολογιών ασφάλειας στον κυβερνοχώρο στις οποίες έχουν πρόσβαση άτομα και 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 **τις διαδικασίες**, 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 στέφθηκαν 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 SOG-IS καλύπτει ένα μέρος μόνο των κρατών μελών της Ένωσης. 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 **και των δηλώσεων συμμόρφωσης ΕΕ** 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 [...] **Ευρωπαϊκά** 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 **διαδικασιών**, προϊόντων και υπηρεσιών ΤΠΕ. Αυτά τα συστήματα θα πρέπει να εφαρμόζονται και να επιβλέπονται από εθνικές [...] αρχές πιστοποίησης **της ασφάλειας στον κυβερνοχώρο** 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 **οι διαδικασίες**, τα προϊόντα και οι υπηρεσίες ΤΠΕ που πιστοποιούνται στο πλαίσιο ενός τέτοιου συστήματος συμμορφώνονται με συγκεκριμένες απαιτήσεις, **με σκοπό [...]** την **[...] προστασία** της διαθεσιμότητας, της αυθεντικότητας, της ακεραιότητας και της εμπιστευτικότητας 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 **καθόλη τη διάρκεια του κύκλου ζωής τους** 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 **διαδικασιών**, των προϊόντων και των υπηρεσιών ΤΠΕ. **Οι διαδικασίες**, 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 συγκεκριμένες **διαδικασίες**, προϊόντα και 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, **στις περιπτώσεις όπου δεν υπάρχουν διαθέσιμα κατάλληλα πρότυπα.**

(55α) Οι τεχνικές προδιαγραφές που θα χρησιμοποιηθούν στο ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο θα πρέπει να προσδιοριστούν τηρώντας τις αρχές που καθορίζονται στο παράρτημα ΙΙ του κανονισμού (ΕΕ) 1025/2012. Ορισμένες αποκλίσεις από τις αρχές αυτές θα μπορούσαν εντούτοις να θεωρηθούν αναγκαίες σε δεόντως αιτιολογημένες περιπτώσεις όταν οι εν λόγω τεχνικές προδιαγραφές πρόκειται να χρησιμοποιηθούν σε ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο αναφερόμενο σε υψηλό επίπεδο διασφάλισης. Οι λόγοι των αποκλίσεων αυτών πρέπει να καθίστανται διαθέσιμοι στο κοινό.

(55β) Η πιστοποιημένη αξιολόγηση της συμμόρφωσης είναι η διαδικασία αξιολόγησης του κατά πόσον πληρούνται οι ειδικές προδιαγραφές που αφορούν μια διαδικασία, ένα προϊόν ή μια υπηρεσία ΤΠΕ. Η διαδικασία αυτή διεξάγεται από ανεξάρτητο τρίτο μέρος, άλλο από τον κατασκευαστή του προϊόντος ή τον πάροχο της υπηρεσίας. Η διαδικασία έκδοσης πιστοποιητικού ακολουθεί τη διαδικασία της επιτυχούς αξιολόγησης της διαδικασίας, του προϊόντος ή της υπηρεσίας ΤΠΕ. Θα πρέπει να θεωρηθεί ως επιβεβαίωση ότι η αντίστοιχη αξιολόγηση έχει διενεργηθεί με σωστό τρόπο. Ανάλογα με το επίπεδο διασφάλισης, το ευρωπαϊκό σύστημα για την ασφάλεια στον κυβερνοχώρο θα πρέπει να προβλέπει αν το πιστοποιητικό εκδίδεται από ιδιωτικό ή δημόσιο φορέα. Η αξιολόγηση της συμμόρφωσης και η πιστοποίηση δεν μπορούν να εγγυηθούν από μόνες τους 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.

(55γ) Η επιλογή, από τους χρήστες των πιστοποιητικών, του κατάλληλου επιπέδου πιστοποίησης και των συναφών απαιτήσεων ασφαλείας θα πρέπει να βασίζεται σε ανάλυση κινδύνου σχετικά με τη χρήση της διαδικασίας, του προϊόντος ή της υπηρεσίας ΤΠΕ. Το επίπεδο διασφάλισης θα πρέπει ως εκ τούτου να είναι ανάλογο με το επίπεδο του κινδύνου που συνδέεται με τη σκοπούμενη χρήση μιας διαδικασίας, ενός προϊόντος ή μιας υπηρεσίας ΤΠΕ.

(55δ) Ένα ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο θα μπορούσε να προβλέπει ότι η αξιολόγηση της συμμόρφωσης πραγματοποιείται υπό την αποκλειστική ευθύνη του κατασκευαστή ή του παρόχου προϊόντων και υπηρεσιών ΤΠΕ (αυτοαξιολόγηση της συμμόρφωσης). Σε αυτές τις περιπτώσεις, αρκεί ο κατασκευαστής ή ο πάροχος να διενεργεί ο ίδιος όλους τους ελέγχους προκειμένου να διασφαλίσει τη συμμόρφωση της διαδικασίας, του προϊόντος ή της υπηρεσίας ΤΠΕ με το σύστημα πιστοποίησης. Αυτό το είδος αξιολόγησης της συμμόρφωσης θα πρέπει να θεωρείται κατάλληλο για τα προϊόντα και τις υπηρεσίες ΤΠΕ χαμηλής πολυπλοκότητας (π.χ. απλοί μηχανισμοί σχεδιασμού και παραγωγής), που ενέχουν χαμηλό κίνδυνο για το δημόσιο συμφέρον. Επιπλέον, μόνο τα προϊόντα και οι υπηρεσίες ΤΠΕ που αντιστοιχούν στο βασικό επίπεδο διασφάλισης θα μπορούσαν να αποτελέσουν αντικείμενο αυτοαξιολόγησης.

(55ε) Ένα ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο θα μπορούσε να επιτρέπει τόσο την πιστοποίηση όσο και την αυτοαξιολόγηση της συμμόρφωσης των προϊόντων και των υπηρεσιών ΤΠΕ. Στην περίπτωση αυτή, το σύστημα θα πρέπει να προβλέπει σαφή και κατανοητά για τους καταναλωτές ή άλλους χρήστες μέσα ώστε να γίνεται διάκριση μεταξύ των προϊόντων και των υπηρεσιών τα οποία αξιολογούνται υπό την ευθύνη του κατασκευαστή ή του παρόχου υπηρεσιών και των προϊόντων και υπηρεσιών που λαμβάνουν πιστοποίηση από τρίτο μέρος.

(55στ) Ο κατασκευαστής ή ο πάροχος προϊόντων και υπηρεσιών ΤΠΕ που προβαίνει σε αυτοαξιολόγηση της συμμόρφωσης θα πρέπει να καταρτίζει και να υπογράφει τη δήλωση συμμόρφωσης ΕΕ στο πλαίσιο της διαδικασίας αξιολόγησης της συμμόρφωσης. Η δήλωση συμμόρφωσης ΕΕ είναι το έγγραφο που αναφέρει ότι ορισμένο προϊόν ή υπηρεσία ΤΠΕ συμμορφώνεται με τις απαιτήσεις του συστήματος. Με την κατάρτιση και την υπογραφή της δήλωσης συμμόρφωσης ΕΕ, ο κατασκευαστής ή ο πάροχος αναλαμβάνει την ευθύνη για τη συμμόρφωση του προϊόντος ή της υπηρεσίας ΤΠΕ με τις νομικές απαιτήσεις του συστήματος. Αντίγραφο της δήλωσης συμμόρφωσης ΕΕ θα πρέπει να υποβάλλεται στην εθνική αρχή πιστοποίησης της ασφάλειας στον κυβερνοχώρο και στον ENISA.

(55ζ) Ο κατασκευαστής ή πάροχος προϊόντων και υπηρεσιών ΤΠΕ θα πρέπει να τηρεί τη δήλωση συμμόρφωσης ΕΕ και την τεχνική τεκμηρίωση όλων των σχετικών πληροφοριών που αφορούν τη συμμόρφωση των προϊόντων ή υπηρεσιών ΤΠΕ με σύστημα το οποίο είναι στη διάθεση της αρμόδιας εθνικής αρχής πιστοποίησης της ασφάλειας στον κυβερνοχώρο για διάστημα που καθορίζεται στο συγκεκριμένο ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο. Ο τεχνικός φάκελος θα πρέπει να προσδιορίζει τις εφαρμοστέες απαιτήσεις και να καλύπτει - στο βαθμό που αυτό απαιτείται για την αξιολόγηση - τον σχεδιασμό, την κατασκευή και τη λειτουργία του προϊόντος ή της υπηρεσίας ΤΠΕ. Η τεχνική τεκμηρίωση θα πρέπει να καταρτίζεται με τρόπο ώστε να είναι δυνατή η αξιολόγηση της συμμόρφωσης ενός προϊόντος ή μιας υπηρεσίας ΤΠΕ με τις σχετικές απαιτήσεις.

(55η) Τα κράτη μέλη και οι ενδιαφερόμενοι φορείς - οργανισμοί θα πρέπει να έχουν το δικαίωμα να προτείνουν στην Ευρωπαϊκή ομάδα πιστοποίησης της ασφάλειας στον κυβερνοχώρο την προετοιμασία ενός υποψήφιου συστήματος. Οι ενδιαφερόμενοι φορείς - οργανισμοί είναι οργανισμοί εκπροσώπων του κλάδου ή των καταναλωτών, συμπεριλαμβανομένων των εκπροσώπων των οργανώσεων των ΜΜΕ, που έχουν εύλογο συμφέρον στην ανάπτυξη ενός ιδιαίτερου ευρωπαϊκού συστήματος πιστοποίησης της ασφάλειας στον κυβερνοχώρο. Οι προτάσεις αυτές θα πρέπει να εξετάζονται σε συνάρτηση με τα κριτήρια που ανέπτυξε η Ευρωπαϊκή ομάδα πιστοποίησης της ασφάλειας στον κυβερνοχώρο δυνάμει των κατευθυντήριων γραμμών με βάση τις αρχές της διαφάνειας, της ανοικτότητας, της αμεροληψίας, της συναίνεσης, της αποτελεσματικότητας, της συνάφειας και της συνοχής.

(56) Η Επιτροπή **και η Ομάδα** θα πρέπει να έχουν τη δυνατότητα να ζητούν από τον ENISA να επεξεργάζεται, **χωρίς αδικαιολόγητη καθυστέρηση,** υποψήφια συστήματα για συγκεκριμένες **διαδικασίες,** προϊόντα ή 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 **διαδικασιών,** προϊόντων και 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 **και τα επίπεδα αξιολόγησης, κατά περίπτωση**.

(56α) Η διασφάλιση ευρωπαϊκού συστήματος πιστοποίησης αποτελεί τη βάση εμπιστοσύνης ότι μια διαδικασία, προϊόν ή υπηρεσία ΤΠΕ πληροί τις απαιτήσεις ασφαλείας συγκεκριμένου ευρωπαϊκού συστήματος πιστοποίησης της ασφάλειας στον κυβερνοχώρο. Προκειμένου να διασφαλισθεί η συνοχή του πλαισίου των πιστοποιημένων διαδικασιών, προϊόντων και υπηρεσιών ΤΠΕ ασφάλειας στον κυβερνοχώρο, ένα ευρωπαϊκό σύστημα πιστοποίησης είναι δυνατόν να προσδιορίζει τα επίπεδα διασφάλισης των ευρωπαϊκών πιστοποιητικών ασφάλειας στον κυβερνοχώρο και τις δηλώσεις συμμόρφωσης ΕΕ που εκδίδονται στο πλαίσιο του εν λόγω συστήματος. Κάθε πιστοποιητικό θα μπορεί να αναφέρεται σε ένα από τα επίπεδα διασφάλισης: βασικό, ουσιαστικό ή υψηλό, ενώ η δήλωση συμμόρφωσης ΕΕ θα μπορεί να αναφέρεται μόνον στο βασικό επίπεδο διασφάλισης. Τα επίπεδα διασφάλισης παρέχουν αντίστοιχο βαθμό προσπαθειών για την αξιολόγηση [...]και χαρακτηρίζονται βάσει σχετικών τεχνικών προδιαγραφών, προτύπων και διαδικασιών, συμπεριλαμβανομένων τεχνικών ελέγχων, σκοπός των οποίων είναι η άμβλυνση ή η πρόληψη συμβάντων που αφορούν την ασφάλεια στον κυβερνοχώρο. Κάθε επίπεδο διασφάλισης πρέπει να είναι συνεπές μεταξύ των διαφόρων τομέων όπου εφαρμόζεται η πιστοποίηση.

(56β) Το ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο μπορεί να προσδιορίζει διάφορα επίπεδα αξιολόγησης ανάλογα με την αυστηρότητα και το βάθος της μεθοδολογίας αξιολόγησης που χρησιμοποιείται και τα οποία θα πρέπει να αντιστοιχούν σε ένα από τα επίπεδα διασφάλισης και να συνδέονται με κατάλληλο συνδυασμό συστατικών στοιχείων διασφάλισης. Για όλα τα επίπεδα διασφάλισης, το προϊόν ή η υπηρεσία ΤΠΕ θα πρέπει να περιλαμβάνουν μια σειρά ασφαλών λειτουργιών, όπως ορίζονται από το σύστημα, στις οποίες μπορούν να περιλαμβάνονται: εξ αρχής ρυθμίσεις ασφαλείας, υπογεγραμμένος κώδικας, ασφαλής επικαιροποίηση/ενημέρωση και περιορισμοί εκμετάλλευσης, καθώς και πλήρεις προστασίες μνήμης σωρού/συστοιχίας. Οι λειτουργίες αυτές θα πρέπει να έχουν αναπτυχθεί και να διατηρούνται με τη χρήση προσεγγίσεων ανάπτυξης και συναφών εργαλείων που επικεντρώνονται στην ασφάλεια κατά τρόπον ώστε να διασφαλίζεται η αξιόπιστη ενσωμάτωση αποτελεσματικών μηχανισμών (τόσο λογισμικού όσο και υλισμικού). Για το βασικό επίπεδο διασφάλισης, η αξιολόγηση πρέπει να καθοδηγείται τουλάχιστον από τα ακόλουθα συστατικά στοιχεία διασφάλισης: η αξιολόγηση θα πρέπει τουλάχιστον να περιλαμβάνει επανεξέταση των τεχνικών τεκμηριώσεων του προϊόντος ή της υπηρεσίας ΤΠΕ την οποία διενεργεί ο οργανισμός αξιολόγησης της συμμόρφωσης. Όταν η πιστοποίηση περιλαμβάνει διαδικασίες ΤΠΕ, θα πρέπει να υπόκειται σε τεχνική επανεξέταση και η μέθοδος που χρησιμοποιείται για τον σχεδιασμό, την ανάπτυξη και τη διατήρηση προϊόντος ή υπηρεσίας ΤΠΕ. Στις περιπτώσεις που ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο προβλέπει αυτοαξιολόγηση της συμμόρφωσης, θα πρέπει να αρκεί αν ο κατασκευαστής ή ο πάροχος έχει προβεί σε αυτοαξιολόγηση της συμμόρφωσης των διαδικασιών, προϊόντων ή υπηρεσιών ΤΠΕ με το σύστημα πιστοποίησης. Για το ουσιαστικό επίπεδο διασφάλισης, η αξιολόγηση θα πρέπει, επιπλέον του βασικού επιπέδου διασφάλισης, να καθοδηγείται τουλάχιστον από την επαλήθευση της συμμόρφωσης των λειτουργιών ασφαλείας του προϊόντος ή της υπηρεσίας ΤΠΕ με την οικεία τεχνική τεκμηρίωση. Για το υψηλό επίπεδο διασφάλισης, η αξιολόγηση θα πρέπει, επιπλέον του ουσιαστικού επιπέδου διασφάλισης, να καθοδηγείται τουλάχιστον από δοκιμή απόδοσης, με την οποία αξιολογείται η ανθεκτικότητα των λειτουργιών ασφαλείας του προϊόντος ή της υπηρεσίας ΤΠΕ έναντι όσων πραγματοποιούν περίτεχνες επιθέσεις στον κυβερνοχώρο και διαθέτουν σημαντικές δεξιότητες και πόρους.

(56γ) Κατά την εκπόνηση υποψήφιου συστήματος, ο ENISA θα πρέπει να διαβουλεύεται με όλους τους σχετικούς άμεσα ενδιαφερομένους, όπως είναι οι ευρωπαϊκοί οργανισμοί τυποποίησης, οι αρμόδιες εθνικές αρχές, οργανισμοί που βασίζονται σε συμφωνίες αμοιβαίας αναγνώρισης όπως η ΣΑΑ SOG-IS, μικρομεσαίες επιχειρήσεις, οργανώσεις καταναλωτών, καθώς και περιβαλλοντικοί και κοινωνικοί φορείς.

(56δ) Ο ENISA θα πρέπει να διατηρεί δικτυακό τόπο που να παρέχει πληροφορίες και δημοσιότητα για τα ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο και να περιλαμβάνει, μεταξύ άλλων, τα αιτήματα για την προετοιμασία υποψήφιου ευρωπαϊκού συστήματος πιστοποίησης της ασφάλειας στον κυβερνοχώρο, καθώς και τις παρατηρήσεις που υποβλήθηκαν κατά τη διαδικασία διαβούλευσης που διενήργησε ο ENISA στη φάση της προετοιμασίας. Ο εν λόγω δικτυακός τόπος θα πρέπει επίσης να παρέχει πληροφορίες σχετικά με τα πιστοποιητικά και τις δηλώσεις συμμόρφωσης ΕΕ που εκδίδονται δυνάμει του παρόντος κανονισμού.

(57) Η προσφυγή στην ευρωπαϊκή πιστοποίηση της ασφάλειας στον κυβερνοχώρο **και στη δήλωση συμμόρφωσης ΕΕ** θα πρέπει να παραμένει εθελοντική, εκτός αν ορίζεται άλλως στην ενωσιακή ή την εθνική νομοθεσία **που έχει εκδοθεί σύμφωνα με το ενωσιακό δίκαιο. Ελλείψει εναρμονισμένης νομοθεσίας, τα κράτη μέλη μπορούν να θεσπίζουν εθνικούς τεχνικούς κανονισμούς σύμφωνα με την οδηγία (ΕΕ) 2015/1535 που προβλέπει υποχρεωτική πιστοποίηση στο πλαίσιο ευρωπαϊκού συστήματος πιστοποίησης της ασφάλειας στον κυβερνοχώρο. Τα κράτη μέλη θα μπορούν επίσης να προσφεύγουν στην ευρωπαϊκή πιστοποίηση της ασφάλειας στον κυβερνοχώρο στο πλαίσιο των δημόσιων συμβάσεων και της οδηγίας 2014/214/ΕΕ**. [...]

(57α) 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 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. Ωστόσο, τα κράτη μέλη δεν θα πρέπει να εμποδίζονται να θεσπίζουν ή να διατηρούν εθνικά συστήματα πιστοποίησης για σκοπούς εθνικής ασφάλειας.

(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 περιορίζουν, να αναστέλλουν ή** 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) [...] Τα κράτη μέλη [...]**θα πρέπει** να ορίζουν μία **ή περισσότερες** [...]**αρχές** πιστοποίησης της ασφάλειας στον κυβερνοχώρο, οι οποίες θα εποπτεύουν τη συμμόρφωση **προς τις υποχρεώσεις που απορρέουν από τον παρόντα κανονισμό. Εάν κράτος μέλος το κρίνει σκόπιμο, τα καθήκοντα μπορούν να ανατεθούν και σε ήδη υπάρχουσες αρχές.**
Τα κράτη μέλη θα πρέπει επίσης να είναι σε θέση να αποφασίζουν, κατόπιν αμοιβαίας συμφωνίας με άλλο κράτος μέλος, για τον ορισμό μιας ή περισσότερων εποπτικών αρχών στην επικράτεια του συγκεκριμένου άλλου κράτους μέλους. Η αρχή οφείλει ιδίως να παρακολουθεί και να εφαρμόζει τις υποχρεώσεις των κατασκευαστών ή των παρόχων προϊόντων και υπηρεσιών ΤΠΕ που είναι εγκατεστημένοι στα αντίστοιχα εδάφη τους σχετικά με τη δήλωση συμμόρφωσης ΕΕ, να επικουρεί τους εθνικούς οργανισμούς διαπίστευσης στην παρακολούθηση και την εποπτεία των δραστηριοτήτων των οργανισμών αξιολόγησης της συμμόρφωσης με την παροχή εμπειρογνωσίας και σχετικών πληροφοριών, να εξουσιοδοτεί τους οργανισμούς αξιολόγησης της συμμόρφωσης για την εκτέλεση των καθηκόντων τους όταν πληρούν τις επιπρόσθετες απαιτήσεις που ορίζονται σε σύστημα και να παρακολουθεί τις σχετικές εξελίξεις στον τομέα της πιστοποίησης της ασφάλειας στον κυβερνοχώρο[...]. Οι εθνικές [...] αρχές πιστοποίησης **της ασφάλειας στον κυβερνοχώρο** θα πρέπει να χειρίζονται τις καταγγελίες που υποβάλλονται από φυσικά ή νομικά πρόσωπα σε σχέση με πιστοποιητικά που έχουν εκδοθεί από **τις ίδιες ή πιστοποιητικά που έχουν εκδοθεί από οργανισμούς αξιολόγησης της συμμόρφωσης αναφερόμενα σε υψηλό επίπεδο διασφάλισης**[...], 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 [...] αρχές πιστοποίησης **της ασφάλειας στον κυβερνοχώρο** 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 **εκπροσώπους των** [...] εθνικών αρχών πιστοποίησης **της ασφάλειας στον κυβερνοχώρο ή άλλων αρμόδιων εθνικών αρχών**. 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 παρέχει συνδρομή 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 **στον Οργανισμό για τα υποψήφια συστήματα και** στην Επιτροπή όσον αφορά τη διατήρηση και την επανεξέταση υφιστάμενων ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο.

(60α) Η Ομάδα οφείλει να διευκολύνει την ανταλλαγή βέλτιστων πρακτικών και εμπειρογνωσίας μεταξύ των εθνικών αρχών πιστοποίησης της ασφάλειας στον κυβερνοχώρο, οι οποίες είναι αρμόδιες για την εξουσιοδότηση των οργανισμών αξιολόγησης της συμμόρφωσης και την έκδοση των πιστοποιητικών. Η Ομάδα θα πρέπει να υποστηρίξει την ανάπτυξη μηχανισμού αξιολόγησης από ομοτίμους στο πλαίσιο της προετοιμασίας υποψήφιου συστήματος και της εφαρμογής του για τους οργανισμούς έκδοσης ευρωπαϊκών πιστοποιητικών ασφάλειας στον κυβερνοχώρο για το υψηλό επίπεδο διασφάλισης. Οι εν λόγω αξιολογήσεις από ομοτίμους θα πρέπει ειδικότερα να αξιολογούν αν οι σχετικοί οργανισμοί διαθέτουν την κατάλληλη εμπειρογνωσία και ασκούν τα καθήκοντά τους με εναρμονισμένο τρόπο. Τα αποτελέσματα των αξιολογήσεων από ομοτίμους θα πρέπει να δημοσιεύονται. Οι οργανισμοί αυτοί μπορούν να λαμβάνουν κατάλληλα μέτρα για να προσαρμόσουν τις πρακτικές και την εμπειρογνωσία τους.

(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.

(61α) Προκειμένου να διευκολυνθεί περαιτέρω το εμπόριο και αναγνωρίζοντας ότι οι αλυσίδες εφοδιασμού ΤΠΕ είναι παγκόσμιες, η Ένωση μπορεί να συνάπτει, σύμφωνα με το άρθρο 218 της ΣΛΕΕ, συμφωνίες αμοιβαίας αναγνώρισης για τα πιστοποιητικά που εκδίδονται από συστήματα θεσπιζόμενα στο πλαίσιο του ευρωπαϊκού πλαισίου πιστοποίησης της ασφάλειας στον κυβερνοχώρο. Η Επιτροπή, λαμβάνοντας υπόψη τις συμβουλές του ENISA και της ομάδας πιστοποίησης της ασφάλειας στον κυβερνοχώρο, δύναται να συστήσει την έναρξη σχετικών διαπραγματεύσεων. Κάθε σύστημα θα πρέπει να προβλέπει ειδικούς όρους αμοιβαίας αναγνώρισης με τις τρίτες χώρες.

(62) [...]

(63) [...]

(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 [...] αρχές πιστοποίησης **της ασφάλειας στον κυβερνοχώρο** 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

1. 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 [...]**Ευρωπαϊκής Ένωσης 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 **διαδικασιών,** 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.

2. **Ο παρών κανονισμός δεν θίγει 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 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 καταστρέψει, να διαταράξει ή να επιδράσει κατ' άλλον τρόπο** 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 **ή την αξιολόγηση της συμμόρφωσης των διαδικασιών,** των προϊόντων και των υπηρεσιών τεχνολογίας των πληροφοριών και των επικοινωνιών (ΤΠΕ) που εμπίπτουν στο πεδίο εφαρμογής του συγκεκριμένου συστήματος·

(9α) «εθνικό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο»: πλήρες σύνολο κανόνων, τεχνικών απαιτήσεων, προτύπων και διαδικασιών το οποίο αναπτύσσεται και εγκρίνεται από εθνική δημόσια αρχή και εφαρμόζεται για την πιστοποίηση ή την αξιολόγηση της συμμόρφωσης των διαδικασιών, των προϊόντων και των υπηρεσιών ΤΠΕ που εμπίπτουν στο πεδίο εφαρμογής του συγκεκριμένου συστήματος·

(10) «ευρωπαϊκό πιστοποιητικό ασφάλειας στον κυβερνοχώρο»: έγγραφο [...] το οποίο βεβαιώνει ότι μια συγκεκριμένη **διαδικασία,** προϊόν ή υπηρεσία ΤΠΕ [...]**έχει αξιολογηθεί ως προς τη συμμόρφωση με** ειδικές απαιτήσεις **ασφαλείας** που προβλέπει ένα ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο·

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

(11α) «υπηρεσία ΤΠΕ»: κάθε υπηρεσία που συνίσταται εξ ολοκλήρου ή κατά κύριο λόγο στη διαβίβαση, αποθήκευση, ανάκτηση ή επεξεργασία πληροφοριών μέσω συστημάτων δικτύου και πληροφοριών·

(11β) «διαδικασία ΤΠΕ»: κάθε σύνολο δραστηριοτήτων που διεξάγονται για να σχεδιάζουν, να αναπτύσσουν, να παρέχουν και να διατηρούν προϊόντα ή υπηρεσίες ΤΠΕ·

(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·

(16α) «τεχνική προδιαγραφή»: έγγραφο με το οποίο ορίζονται τα απαιτούμενα τεχνικά χαρακτηριστικά διαδικασίας, προϊόντος ή υπηρεσίας ΤΠΕ·

(16β) «επίπεδο διασφάλισης»: η βάση εμπιστοσύνης ότι μια διαδικασία, προϊόν ή υπηρεσία ΤΠΕ πληροί τις απαιτήσεις ασφαλείας συγκεκριμένου ευρωπαϊκού συστήματος πιστοποίησης της ασφάλειας στον κυβερνοχώρο και το επίπεδο στο οποίο έχει αξιολογηθεί· το επίπεδο διασφάλισης δεν μετρά την ασφάλεια των ίδιων των διαδικασιών, προϊόντων ή υπηρεσιών ΤΠΕ.

ΤΙΤΛΟΣ ΙΙ

ENISA – ο «Οργανισμός*[...]της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο*»

ΚΕΦΑΛΑΙΟ Ι

ΕΝΤΟΛΗ ΚΑΙ ΣΤΟΧΟΙ*[...]*

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 [...] **σε ολόκληρη** την Ένωση**, ιδίως υποστηρίζοντας τα κράτη μέλη, τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης για τη βελτίωση της ασφάλειας στον κυβερνοχώρο. Ο Οργανισμός ενεργεί ως σημείο αναφοράς των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης για συμβουλές και εμπειρογνωσία σχετικά με την ασφάλεια στον κυβερνοχώρο.**

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.

2α. Κατά την εκτέλεση των καθηκόντων του, ο Οργανισμός ενεργεί ανεξάρτητα και λαμβάνει στον μέγιστο βαθμό υπόψη την εμπειρογνωσία των αρμόδιων αρχών των κρατών μελών, αποφεύγοντας παράλληλα την επικάλυψη δραστηριοτήτων.

3. [...]

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 **της Ένωσης** που σχετίζονται με την ασφάλεια στον κυβερνοχώρο**, συμπεριλαμβανομένων των τομεακών πολιτικών για την ασφάλεια στον κυβερνοχώρο**.

3. Ο Οργανισμός στηρίζει την ανάπτυξη ικανοτήτων και την ετοιμότητα στην Ένωση, επικουρώντας **τα θεσμικά και λοιπά όργανα και οργανισμούς** της Ένωσης, **καθώς και** τα κράτη μέλη και τους ιδιωτικούς και δημόσιους άμεσα ενδιαφερόμενους, με σκοπό την ενίσχυση της προστασίας των συστημάτων δικτύου και πληροφοριών τους, την ανάπτυξη **και τη βελτίωση της ανθεκτικότητας στον κυβερνοχώρο και της ικανότητας ανταπόκρισης και την ανάπτυξη** δεξιοτήτων και ικανοτήτων στο πεδίο της ασφάλειας 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 **ιδιωτικούς και δημόσιους** άμεσα ενδιαφερόμενους[...] σε θέματα που σχετίζονται με την ασφάλεια στον κυβερνοχώρο.

5. Ο Οργανισμός **συμβάλλει στην αύξηση** [...]των δυνατοτήτων ασφάλειας στον κυβερνοχώρο σε επίπεδο Ένωσης προκειμένου να [...]**επικουρεί** τα κράτη μέλη όσον αφορά την πρόληψη και την αντιμετώπιση απειλών στον κυβερνοχώρο, κυρίως σε περίπτωση διασυνοριακών συμβάντων.

6. Ο Οργανισμός προάγει τη χρήση της πιστοποίησης **προκειμένου να αποφευχθεί ο κατακερματισμός των συστημάτων πιστοποίησης στην ΕΕ. Ειδικότερα, ο Οργανισμός συμβάλλει** [...] 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.

ΚΕΦΑΛΑΙΟ ΙΑ
ΚΑΘΗΚΟΝΤΑ

Άρθρο 5

*[...]**Χάραξη και 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 [...] **συμβάντων σχετικά με την** ασφάλεια 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

*[...]**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 [...] **απειλών**[...] 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 [...] **απειλών**[...] και συμβάντων σχετικών με την ασφάλεια στον κυβερνοχώρο, **ιδίως** 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 των 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 **τακτικών** [...] 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, **στην** [...]ανταλλαγή [...]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 **στηρίζει την ανταλλαγή πληροφοριών στους τομείς και μεταξύ των τομέων**[...], 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

*[...]**Επιχειρησιακή συνεργασία σε επίπεδο Ένωσης***

1. Ο Οργανισμός υποστηρίζει την επιχειρησιακή συνεργασία μεταξύ **κρατών μελών, των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης** [...] 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**, σε αυτό το πλαίσιο,** διευκολύνει [...]την ανταλλαγή πληροφοριών και τη συνεργασία μεταξύ των μελών του.

4. Ο Οργανισμός **στηρίζει** [...]την επιχειρησιακή συνεργασία εντός του δικτύου CSIRT εξασφαλίζοντας στήριξη στα κράτη μέλη **- κατόπιν αιτήματός τους,** με:

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

β) [...]**διευκόλυνση της** τεχνικής **διαχείρισης**[...] περιστατικών που έχουν σημαντικό ή ουσιαστικό αντίκτυπο**, ιδίως, μεταξύ άλλων, με στήριξη της εθελοντικής ανταλλαγής τεχνικών λύσεων μεταξύ των κρατών μελών**·

γ) την ανάλυση τρωτών σημείων[...] και συμβάντων·

γα) την παροχή στήριξης σε τεχνικές εκ των υστέρων έρευνες σχετικά με συμβάντα με σημαντικό ή ουσιαστικό αντίκτυπο σύμφωνα με την οδηγία (ΕΕ) 2016/1148.

Κατά την εκτέλεση αυτών των καθηκόντων, ο Οργανισμός και η CERT-EU δεσμεύονται σε μια δομημένη συνεργασία προκειμένου να επωφελούνται από τις συνέργειες **και να αποφεύγεται η αλληλεπικάλυψη δραστηριοτήτων**[...].

5. [...]

[...]

6. Ο Οργανισμός οργανώνει **τακτικές** [...]ασκήσεις ασφάλειας στον κυβερνοχώρο σε επίπεδο Ένωσης και παρέχει συνδρομή σε όλα τα κράτη μέλη και τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ στην οργάνωση ασκήσεων κατόπιν αιτήματός (αιτημάτων) τους. **Οι εν λόγω ασκήσεις σε επίπεδο Ένωσης είναι δυνατόν να περιλαμβάνουν τεχνικά, επιχειρησιακά και στρατηγικά στοιχεία**[...]. **Άπαξ ανά διετία διοργανώνεται άσκηση μεγάλης κλίμακας περιέχουσα όλα αυτά τα στοιχεία.** Επιπλέον, ο Οργανισμός συμβάλλει και επικουρεί τη διοργάνωση, αν κρίνεται σκόπιμο, των τομεακών ασκήσεων ασφάλειας στον κυβερνοχώρο μαζί με αρμόδιους [...]**οργανισμούς που μπορούν** να συμμετέχουν επίσης **στις** ασκήσεις ασφάλειας στον κυβερνοχώρο σε επίπεδο Ένωσης.

7. Ο Οργανισμός εκπονεί**, σε στενή συνεργασία με τα κράτη μέλη,** 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 [...] ή τα ενιαία κέντρα επαφής της οδηγίας για την ασφάλεια δικτύων και πληροφοριών (**αμφότερα εθελοντικώς**[...])· 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 **με εθελοντικές ανταλλαγές** 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) [...]**κατόπιν αιτήματος κρατών μελών, τη διευκόλυνση** της τεχνικής διαχείρισης περιστατικού ή κρίσεως, **ιδίως,** μεταξύ άλλων[...]**με στήριξη** της **εθελοντικής** ανταλλαγής τεχνικών λύσεων μεταξύ των κρατών μελών;

δ) τη στήριξη **των θεσμικών και λοιπών οργάνων και των οργανισμών της ΕΕ, και, εφόσον ζητηθεί, των κρατών μελών στη** δημόσια επικοινωνία σχετικά με το συμβάν ή την κρίση·

ε) **τη στήριξη των κρατών μελών, εφόσον το ζητήσουν, στη** δοκιμασία των προγραμμάτων συνεργασίας για την αντιμετώπιση τέτοιων συμβάντων ή κρίσεων.

Άρθρο 8

*[...]**Αγορά, πιστοποίηση της ασφάλειας στον κυβερνοχώρο και προτυποποίηση***

Ο Οργανισμός:

α) υποστηρίζει και προάγει τη χάραξη και την εφαρμογή της πολιτικής της Ένωσης για την πιστοποίηση της ασφάλειας στον κυβερνοχώρο για **διαδικασίες,** 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 **διαδικασίες,** προϊόντα και υπηρεσίες ΤΠΕ, **σε συνεργασία με τον κλάδο και** 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 [...]αρχές πιστοποίησης **στον κυβερνοχώρο** και τη βιομηχανία·

(3α) συνιστώντας κατάλληλες τεχνικές προδιαγραφές για τη χρήση της ανάπτυξης ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο όπως αναφέρεται στο άρθρο 47 παράγραφος 1 στοιχείο β) σε περιπτώσεις στις οποίες δεν υπάρχουν διαθέσιμα πρότυπα·

(3β) συμβάλλοντας στην επαρκή ανάπτυξη ικανοτήτων σχετικά με διαδικασίες αξιολόγησης και πιστοποίησης με τη συγκέντρωση και τη δημοσίευση κατευθυντηρίων γραμμών, καθώς και με την παροχή στήριξης σε κράτη μέλη κατόπιν αιτήματός τους·

β) διευκολύνει την καθιέρωση και χρήση ευρωπαϊκών και διεθνών προτύπων για τη διαχείριση κινδύνου και την ασφάλεια των **διαδικασιών,** προϊόντων και [...] υπηρεσιών ΤΠΕ·

βα) εκπονεί, σε συνεργασία με τα κράτη μέλη, συμβουλές και κατευθυντήριες γραμμές 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

*[...]**Γνώση* και *πληροφορίες***[...]

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[...] **συμβάντων** σχετικών 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 [...]των υποδομών που υποστηρίζουν τους τομείς που αναφέρονται στο παράρτημα ΙΙ της οδηγίας (ΕΕ) 2016/1148 **και των χρησιμοποιούμενων από τους παρόχους ψηφιακών υπηρεσιών που αναφέρονται στον κατάλογο του παραρτήματος ΙΙΙ της εν λόγω οδηγίας**·

δ) συγκεντρώνει, οργανώνει και γνωστοποιεί στο κοινό, μέσω ειδικής πύλης, πληροφορίες σχετικά με την ασφάλεια στον κυβερνοχώρο, τις οποίες παρέχουν τα θεσμικά και λοιπά όργανα και οι οργανισμοί της Ένωσης **και, εθελοντικώς, τα κράτη μέλη και ιδιωτικοί και δημόσιοι άμεσα ενδιαφερόμενοι**·

ε) [...]

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) [...].

Άρθρο 9α

Ευαισθητοποίηση και εκπαίδευση

Ο Οργανισμός:

α) 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·

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

γ) επικουρεί τα κράτη μέλη στις προσπάθειές τους να αυξήσουν την ευαισθητοποίηση για την ασφάλεια στον κυβερνοχώρο και να προαγάγουν την εκπαίδευση για την ασφάλεια στον κυβερνοχώρο·

δ) στηρίζει τη στενότερη συνεργασία και την ανταλλαγή βέλτιστων πρακτικών μεταξύ των κρατών μελών όσον αφορά την εκπαίδευση και την ευαισθητοποίηση για την ασφάλεια στον κυβερνοχώρο, διευκολύνοντας τη δημιουργία και τη διατήρηση ενός δικτύου εθνικών εκπαιδευτικών σημείων επαφής.

Άρθρο 10

*[...]**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

*[...]**Διεθνής 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, [...]**εντός των σχετικών πλαισίων διεθνούς συνεργασίας**, την ανταλλαγή βέλτιστων πρακτικών[...]·

γ) παρέχοντας, κατόπιν αιτήματος, εμπειρογνωσία στην Επιτροπή·

γα) σε συνεργασία με την ευρωπαϊκή ομάδα πιστοποίησης της ασφάλειας στον κυβερνοχώρο που θεσπίστηκε βάσει του άρθρου 53 και παρέχει συμβουλές και στήριξη προς την Επιτροπή σε θέματα σχετικά με συμφωνίες για την αμοιβαία αναγνώριση των πιστοποιητικών ασφάλειας στον κυβερνοχώρο με τρίτες χώρες.

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·[...]

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

δα) δίκτυο εθνικών υπαλλήλων-συνδέσμων, το οποίο ασκεί τις αρμοδιότητες που καθορίζονται στο άρθρο 20α.

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·

γα) επιβλέπει την εφαρμογή του πολυετούς και του ετήσιου προγραμματισμού που περιλαμβάνεται στο ενιαίο έγγραφο προγραμματισμού·

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 απωλέσουν 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. [...]

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 **περιλαμβανομένης της υλοποίησης του ετήσιου προγράμματος εργασίας** 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·

ιβ-α) την τακτική επικοινωνία με τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ σχετικά με τις δραστηριότητές τους στον τομέα της ασφάλειας στον κυβερνοχώρο προκειμένου να διασφαλίζεται η συνεκτικότητα κατά την ανάπτυξη και εφαρμογή της πολιτικής της ΕΕ·

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. **Όποτε απαιτείται, για την αποτελεσματική και επαρκή άσκηση των καθηκόντων του Οργανισμού και με βάση κατάλληλη ανάλυση κόστους-οφέλους, ο** εκτελεστικός διευθυντής **μπορεί** να αποφασίσει [...]**την εγκαθίδρυση ενός ή περισσότερων τοπικών γραφείων σε ένα ή περισσότερα κράτη μέλη**. Προτού λάβει απόφαση για εγκαθίδρυση τοπικού γραφείου, ο εκτελεστικός διευθυντής **ζητεί τη γνώμη του οικείου κράτους μέλους ή των οικείων κρατών μελών, συμπεριλαμβανομένου του κράτους μέλους όπου βρίσκεται η έδρα του Οργανισμού, και** λαμβάνει εκ των προτέρων τη συγκατάθεση της Επιτροπής **και** του διοικητικού συμβουλίου[...]. **Σε περίπτωση διαφωνίας κατά τη διαδικασία διαβούλευσης μεταξύ του εκτελεστικού διευθυντή και των οικείων κρατών μελών, το θέμα τίθεται προς συζήτηση στο Συμβούλιο.** 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.[...] **Ο αριθμός των μελών του προσωπικού σε όλα τα τοπικά γραφεία θα είναι ο ελάχιστος απαιτούμενος και δεν θα υπερβαίνει στο σύνολό του το 40 % του [...] προσωπικού που βρίσκεται στο κράτος μέλος όπου βρίσκεται η έδρα του Οργανισμού. Ο αριθμός των μελών του προσωπικού σε κάθε τοπικό γραφείο δεν θα υπερβαίνει το 10 % του [...] αριθμού των μελών του [...] προσωπικού που βρίσκεται στο κράτος μέλος όπου βρίσκεται η έδρα του Οργανισμού.**

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, **τους φορείς εκμετάλλευσης βασικών υπηρεσιών,** 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.

5α. Η μόνιμη ομάδα ενδιαφερομένων πρέπει να ενημερώνει τακτικά το διοικητικό συμβούλιο για τις δραστηριότητές της.

ΤΜΗΜΑ 4Α

ΔΙΚΤΥΟ ΕΘΝΙΚΩΝ ΥΠΑΛΛΗΛΩΝ-ΣΥΝΔΕΣΜΩΝ

Άρθρο 20α

Δίκτυο εθνικών υπαλλήλων-συνδέσμων

1. Το διοικητικό συμβούλιο, ενεργώντας κατόπιν πρότασης του εκτελεστικού διευθυντή, συγκροτεί δίκτυο εθνικών υπαλλήλων-συνδέσμων, αποτελούμενο από εκπροσώπους των κρατών μελών.

2. Το δίκτυο εθνικών υπαλλήλων-συνδέσμων αποτελείται από εκπροσώπους όλων των κρατών μελών. Κάθε κράτος μέλος ορίζει έναν εκπρόσωπο. Οι συνεδριάσεις του δικτύου μπορούν να διεξάγονται με διάφορες συνθέσεις εμπειρογνωμόνων.

3. Το δίκτυο εθνικών υπαλλήλων-συνδέσμων διευκολύνει ιδίως την ανταλλαγή πληροφοριών μεταξύ του ENISA και των κρατών μελών. Ειδικότερα, υποστηρίζει τον ENISA για τη διάδοση των δραστηριοτήτων του, των πορισμάτων του και των συστάσεών του στο σύνολο της ΕΕ, με αποδέκτες τους σχετικούς άμεσα ενδιαφερόμενους.

4. Οι εθνικοί υπάλληλοι-σύνδεσμοι ενεργούν ως κεντρικά σημεία επαφής σε εθνικό επίπεδο ώστε να διευκολύνεται η συνεργασία μεταξύ του ENISA και των εθνικών εμπειρογνωμόνων στο πλαίσιο της υλοποίησης του προγράμματος εργασίας του ENISA.

5. Οι εθνικοί υπάλληλοι-σύνδεσμοι θα πρέπει να συνεργάζονται στενά με τους εκπροσώπους των χωρών τους στο διοικητικό συμβούλιο, ωστόσο, το έργο του δικτύου δεν θα πρέπει να επικαλύπτει το έργο του διοικητικού συμβουλίου ή άλλων φορέων της ΕΕ.

6. Οι αρμοδιότητες και οι διαδικασίες για το εθνικό δίκτυο υπαλλήλων-συνδέσμων προσδιορίζονται στους εσωτερικούς κανόνες λειτουργίας του Οργανισμού και δημοσιοποιούνται.

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

---

14 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)

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

Εμπιστευτικότητα

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[15] και στην απόφαση (ΕΚ, Ευρατόμ) 2015/444 της Επιτροπής[16]. Οι κανόνες αυτοί περιλαμβάνουν διατάξεις που έχουν σχέση με την ανταλλαγή, την επεξεργασία και την αποθήκευση διαβαθμισμένων πληροφοριών.

---

15 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).

16 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).

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.

ΚΕΦΑΛΑΙΟ III
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[17], 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.

---

17 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).

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[18], 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 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.

[18] 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).

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 **τετραετής** [...]. 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 **τετραετία**[...].

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[...].

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[...].

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[19]. 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[20].

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.

---

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

20 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).

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

Άρθρο 40

Κανόνες ασφαλείας 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 συνθήκες 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 [...] 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 III
ΠΛΑΙΣΙΟ ΠΙΣΤΟΠΟΙΗΣΗΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Άρθρο 43

Ευρωπαϊκό πλαίσιο πιστοποίησης της ασφάλειας στον κυβερνοχώρο [...]

1. **Το ευρωπαϊκό πλαίσιο πιστοποίησης της ασφάλειας στον κυβερνοχώρο αποσκοπεί στη βελτίωση των συνθηκών για τη λειτουργία της εσωτερικής αγοράς διά της αναβάθμισης του επιπέδου ασφάλειας στον κυβερνοχώρο εντός της Ένωσης. Προβλέπει την απαιτούμενη διακυβέρνηση για μια εναρμονισμένη προσέγγιση σε επίπεδο ΕΕ όσον αφορά τα ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο, με απώτερο στόχο τη δημιουργία ψηφιακής ενιαίας αγοράς για τις διαδικασίες, τα προϊόντα και τις υπηρεσίες στον τομέα των ΤΠΕ.**

2. **Το ευρωπαϊκό πλαίσιο πιστοποίησης της ασφάλειας στον κυβερνοχώρο προβλέπει έναν μηχανισμό μέσω του οποίου να θεσπίζονται** [...] ευρωπαϊκ**ά** συστήματ**α** πιστοποίησης της ασφάλειας στον κυβερνοχώρο [...] **και να** βεβαιώνεται ότι **οι διαδικασίες,** τα προϊόντα και οι υπηρεσίες ΤΠΕ που έχουν [...] **αξιολογηθεί** σύμφωνα με τα εν λόγω συστήμα**τα** συμμορφώνονται με συγκεκριμένες απαιτήσεις **ασφάλεια**ς [...] **με σκοπό να διαφυλάσσεται** η διαθεσιμότητα, η γνησιότητα, η ακεραιότητα ή η 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 **και** υπηρεσιών [...] **σε όλη τη διάρκεια του κύκλου ζωής τους**.

Άρθρο 44

Επεξεργασία και έγκριση ενός ευρωπαϊκού συστήματος πιστοποίησης της ασφάλειας στον κυβερνοχώρο

1. Κατόπιν αιτήματος της Επιτροπής **ή της ευρωπαϊκής ομάδας πιστοποίησης της ασφάλειας στον κυβερνοχώρο (εφεξής η «Ομάδα») που συστήνεται δυνάμει του άρθρου 53**, 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. [...]

1α. Τα κράτη μέλη ή οι οργανώσεις ενδιαφερόμενων φορέων μπορούν να προτείνουν στην Ομάδα την επεξεργασία υποψήφιου ευρωπαϊκού συστήματος πιστοποίησης της ασφάλειας στον κυβερνοχώρο. Η Ομάδα αξιολογεί τις εν λόγω προτάσεις βάσει κριτηρίων που καθορίζει η Ομάδα μέσω κατευθυντήριων γραμμών σύμφωνα με το άρθρο 53 παράγραφος 3 στοιχείο γα), και μπορεί να ζητήσει από τον ENISA την επεξεργασία 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 διαβουλεύεται με όλους τους σχετικούς ενδιαφερομένους **μέσω διαφανών διαδικασιών διαβούλευσης** και συνεργάζεται στενά με την Ομάδα. Η Ομάδα παρέχει στον ENISA τη συνδρομή και την εμπειρογνωσία [...] σε σχέση με την επεξεργασία του υποψήφιου συστήματος **και εκδίδει γνώμη σχετικά με το υποψήφιο σύστημα πριν από την υποβολή του στην Επιτροπή** [...]. **Ο ENISA διασφαλίζει ότι τα υποψήφια συστήματα είναι σύμφωνα με το εφαρμοστέο εναρμονισμένο πρότυπο που χρησιμοποιείται για τη διαπίστευση του οργανισμού αξιολόγησης της συμμόρφωσης.**

3. Ο ENISA **λαμβάνει ιδιαιτέρως υπόψη τη γνώμη της Ομάδας προτού να διαβιβάσει** στην Επιτροπή [...] το υποψήφιο [...] σύστημα που επεξεργάστηκε σύμφωνα 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 2, οι οποίες προβλέπουν σε σχέση με ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο **διαδικασίες,** προϊόντα και υπηρεσίες ΤΠΕ που πληρούν τις απαιτήσεις των άρθρων 45, 46 και 47 του παρόντος κανονισμού.

5. [...]

Άρθρο 44α

Διατήρηση ευρωπαϊκού συστήματος πιστοποίησης της ασφάλειας στον κυβερνοχώρο

1. Ο Οργανισμός διατηρεί έναν ειδικό δικτυακό τόπο που παρέχει πληροφορίες και εξασφαλίζει την προβολή για τα ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο, τα πιστοποιητικά και τις δηλώσεις συμμόρφωσης ΕΕ που εκδίδονται σύμφωνα με το άρθρο 47α.

2. Ο Οργανισμός, σε στενή συνεργασία με την Ομάδα, επανεξετάζει τουλάχιστον κάθε 5 έτη τα εγκριθέντα ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο λαμβάνοντας υπόψη τις παρατηρήσεις που λαμβάνει από ενδιαφερόμενα μέρη. Εάν κριθεί αναγκαίο, η Επιτροπή ή η Ομάδα μπορεί να ζητήσει από τον Οργανισμό να ξεκινήσει τη διαδικασία ανάπτυξης αναθεωρημένου υποψήφιου συστήματος σύμφωνα με το άρθρο 44 παράγραφοι 2 και 3.

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 [...] **επιτυγχάνει**, κατά περίπτωση, **τουλάχιστον** τους ακόλουθους στόχους ασφάλειας:

α) την προστασία δεδομένων που έχουν αποθηκευτεί, διαβιβαστεί ή αποτελέσει με άλλον τρόπο αντικείμενο επεξεργασίας από τυχαία ή μη εγκεκριμένη αποθήκευση, επεξεργασία, πρόσβαση ή αποκάλυψη, **κατά τη διάρκεια ολόκληρου το κύκλου ζωής της διαδικασίας, του προϊόντος ή της υπηρεσίας**·

β) την προστασία δεδομένων που έχουν αποθηκευτεί, διαβιβαστεί ή αποτελέσει με άλλον τρόπο αντικείμενο επεξεργασίας από τυχαία ή μη εγκεκριμένη καταστροφή, [...] απώλεια ή αλλοίωση **ή έλλειψη διαθεσιμότητας κατά τη διάρκεια ολόκληρου το κύκλου ζωής της διαδικασίας, του προϊόντος ή της υπηρεσίας**·

γ) [...] 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 [...] **στα οποία πραγματοποιήθηκε πρόσβαση, τα οποία χρησιμοποιήθηκαν ή αποτέλεσαν με άλλον τρόπο αντικείμενο επεξεργασίας**, καθώς και του πότε και από ποιον·

ε) [...] τη δυνατότητα να ελέγχεται σε ποια δεδομένα, υπηρεσίες ή λειτουργίες πραγματοποιήθηκε πρόσβαση**,** [...] ποια χρησιμοποιήθηκαν **ή αποτέλεσαν με άλλον τρόπο αντικείμενο επεξεργασίας**, 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) [...] **οι διαδικασίες**, τα προϊόντα και οι υπηρεσίες ΤΠΕ παρέχονται με επικαιροποιημένο λογισμικό **και υλισμικό** που δεν [...] περιέχ**ουν γνωστά στο κοινό** τρωτά σημεία, και προβλέπονται μηχανισμοί για ασφαλείς [...] επικαιροποιήσεις·

ζα) οι διαδικασίες, τα προϊόντα και οι υπηρεσίες ΤΠΕ αναπτύσσονται, κατασκευάζονται και παρέχονται σύμφωνα με τις απαιτήσεις ασφάλειας που ορίζονται στο εκάστοτε σύστημα.

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 **διαδικασίες,** προϊόντα και υπηρεσίες ΤΠΕ [...]. **Το επίπεδο διασφάλισης είναι ανάλογο του επιπέδου του κινδύνου που συνδέεται με την προβλεπόμενη χρήση διαδικασίας, προϊόντος ή υπηρεσίας ΤΠΕ.**

2. Το βασικό, το σημαντικό και το υψηλό επίπεδο διασφάλισης [...] **αναφέρονται σε πιστοποιητικό ή δήλωση συμμόρφωσης ΕΕ που εκδίδεται στο πλαίσιο ευρωπαϊκού συστήματος πιστοποίησης της ασφάλειας στον κυβερνοχώρο και προβλέπει για κάθε επίπεδο διασφάλισης αντίστοιχες απαιτήσεις ασφάλειας συμπεριλαμβανομένων λειτουργιών ασφάλειας και τον αντίστοιχο βαθμό προσπάθειας για την αξιολόγηση διαδικασίας, προϊόντος ή υπηρεσίας ΤΠΕ. Στο πιστοποιητικό ή τη δήλωση συμμόρφωσης ΕΕ αποδίδεται χαρακτηρισμός βάσει τεχνικών προδιαγραφών, προτύπων και διαδικασιών που σχετίζονται με το εν λόγω πιστοποιητικό ή δήλωση, συμπεριλαμβανομένων των τεχνικών ελέγχων, σκοπός των οποίων είναι η μείωση του κινδύνου συμβάντων που αφορούν την ασφάλεια στον κυβερνοχώρο ή η πρόληψή τους ως ακολούθως:**

α) **ένα ευρωπαϊκό πιστοποιητικό ασφάλειας στον κυβερνοχώρο ή μια δήλωση συμμόρφωσης ΕΕ που αναφέρεται σε** «βασικό» επίπεδο διασφάλισης **παρέχει τη διασφάλιση ότι οι διαδικασίες, τα προϊόντα και οι υπηρεσίες ΤΠΕ πληρούν τις αντίστοιχες απαιτήσεις ασφάλειας, συμπεριλαμβανομένων των λειτουργιών ασφάλειας, και έχουν αξιολογηθεί ως προς ένα επίπεδο που έχει ως στόχο την ελαχιστοποίηση των γνωστών βασικών κινδύνων για συμβάντα και επιθέσεις στον κυβερνοχώρο. Οι δραστηριότητες αξιολόγησης περιλαμβάνουν τουλάχιστον την αξιολόγηση της τεχνικής τεκμηρίωσης ή, κατά περίπτωση, περιλαμβάνουν υποκατάστατες δραστηριότητες με ισοδύναμο αποτέλεσμα**[...]·

β) **ένα ευρωπαϊκό πιστοποιητικό ασφάλειας στον κυβερνοχώρο που αναφέρεται σε** «σημαντικό» επίπεδο διασφάλισης **παρέχει τη διασφάλιση ότι οι διαδικασίες, τα προϊόντα και οι υπηρεσίες ΤΠΕ πληρούν τις αντίστοιχες απαιτήσεις ασφάλειας, συμπεριλαμβανομένων των λειτουργιών ασφάλειας, και έχουν αξιολογηθεί ως προς ένα επίπεδο που έχει ως στόχο την ελαχιστοποίηση των γνωστών κινδύνων, συμβάντων και επιθέσεων στον κυβερνοχώρο που πραγματοποιούνται από δράστες με περιορισμένες δεξιότητες και πόρους. Οι δραστηριότητες αξιολόγησης περιλαμβάνουν τουλάχιστον τα εξής: επανεξέταση της μη εφαρμοσιμότητας γνωστών στο κοινό τρωτών σημείων και επαλήθευση ότι οι διαδικασίες, τα προϊόντα και οι υπηρεσίες ΤΠΕ εφαρμόζουν ορθά την αναγκαία λειτουργία ασφάλειας· ή, κατά περίπτωση, περιλαμβάνουν υποκατάστατες δραστηριότητες με ισοδύναμο αποτέλεσμα** [...]·

γ) **ένα ευρωπαϊκό πιστοποιητικό ασφάλειας στον κυβερνοχώρο που αναφέρεται σε** «υψηλό» επίπεδο διασφάλισης **παρέχει τη διασφάλιση ότι οι διαδικασίες, τα προϊόντα και οι υπηρεσίες ΤΠΕ πληρούν τις αντίστοιχες απαιτήσεις ασφάλειας, συμπεριλαμβανομένων των λειτουργιών ασφάλειας, και έχουν αξιολογηθεί ως προς ένα επίπεδο που έχει ως στόχο την ελαχιστοποίηση του κινδύνου επιθέσεων στον κυβερνοχώρο προηγμένης τεχνολογίας που πραγματοποιούνται από δράστες με σημαντικές δεξιότητες και πόρους. Οι δραστηριότητες αξιολόγησης περιλαμβάνουν τουλάχιστον τα εξής: επανεξέταση της μη εφαρμοσιμότητας γνωστών στο κοινό τρωτών σημείων, επαλήθευση ότι οι διαδικασίες, τα προϊόντα και οι υπηρεσίες ΤΠΕ εφαρμόζουν ορθά την αναγκαία λειτουργία ασφάλειας προηγμένης τεχνολογίας, και εκτίμηση της ανθεκτικότητάς τους σε επιδέξιους επιτιθέμενους μέσω δοκιμών διείσδυσης· ή, κατά περίπτωση, περιλαμβάνουν υποκατάστατες δραστηριότητες με ισοδύναμο αποτέλεσμα** [...].

2α. Ένα ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο μπορεί να προσδιορίζει διάφορα επίπεδα αξιολόγησης ανάλογα με την αυστηρότητα και το βάθος της μεθοδολογίας αξιολόγησης. Καθένα από τα επίπεδα αξιολόγησης αντιστοιχεί σε ένα από τα επίπεδα διασφάλισης και ορίζεται από κατάλληλο συνδυασμό συστατικών διασφάλισης.

Άρθρο 47

Στοιχεία των ευρωπαϊκών συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο

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

α) το αντικείμενο και το πεδίο εφαρμογής του **συστήματος** πιστοποίησης, συμπεριλαμβανομένων του τύπου ή των κατηγοριών των καλυπτόμενων **διαδικασιών,** προϊόντων και υπηρεσιών ΤΠΕ, **καθώς και περιγραφή του τρόπου με τον οποίον το σύστημα πιστοποίησης ανταποκρίνεται στις ανάγκες των προσδοκώμενων ομάδων-στόχου**·

β) [...] αναφορά σε [...] διεθνή**, ευρωπαϊκά ή εθνικά** πρότυπα **[...] που εφαρμόζονται κατά την αξιολόγηση. Όταν δεν υπάρχουν πρότυπα, γίνεται αναφορά σε** [...] τεχνικές προδιαγραφές **που πληρούν τις απαιτήσεις του παραρτήματος ΙΙ του κανονισμού 1025/2012 ή, εάν δεν υπάρχουν τέτοιες προδιαγραφές, σε τεχνικές προδιαγραφές ή άλλες απαιτήσεις ασφάλειας στον κυβερνοχώρο που ορίζονται στο σύστημα**·

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

γα) κατά περίπτωση, τις ειδικές ή πρόσθετες απαιτήσεις που εφαρμόζονται σε οργανισμούς αξιολόγησης της συμμόρφωσης προκειμένου να διασφαλίζεται η τεχνική ικανότητά τους να αξιολογούν τις απαιτήσεις ασφάλειας στον κυβερνοχώρο·

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) **κατά περίπτωση,** τις πληροφορίες που παρέχονται **ή άλλως τίθενται στη διάθεση** των οργανισμών 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) [...] τους κανόνες παρακολούθησης της συμμόρφωσης με τις απαιτήσεις των πιστοποιητικών **ή της δήλωσης συμμόρφωσης ΕΕ**, συμπεριλαμβανομένων των μηχανισμών για την κατάδειξη της συνεχούς συμμόρφωσης με τις συγκεκριμένες απαιτήσεις της ασφάλειας στον κυβερνοχώρο·

η) **κατά περίπτωση,** τις προϋποθέσεις για τη χορήγηση **και την ανανέωση πιστοποιητικού**, **καθώς και για** τη διατήρηση, τη συνέχιση, την επέκταση **ή** τον περιορισμό του πεδίου εφαρμογής της πιστοποίησης·

θ) τους κανόνες σχετικά με τις συνέπειες της μη συμμόρφωσης των πιστοποιημένων **ή αυτοαξιολογούμενων** προϊόντων και υπηρεσιών ΤΠΕ με τις απαιτήσεις [...] **του συστήματος**·

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

ια) **κατά περίπτωση,** τους κανόνες σχετικά με την τήρηση μητρώων από τους οργανισμούς αξιολόγησης της συμμόρφωσης·

ιβ) τον προσδιορισμό εθνικών **ή διεθνών** συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο που καλύπτουν τον ίδιο τύπο ή τις ίδιες κατηγορίες **διαδικασιών,** προϊόντων και υπηρεσιών ΤΠΕ**, απαιτήσεις ασφάλειας και κριτήρια και μεθόδους αξιολόγησης**·

ιγ) το περιεχόμενο του εκδιδόμενου πιστοποιητικού **ή της δήλωσης συμμόρφωσης ΕΕ·**

ιγ-α) την περίοδο αποθήκευσης της δήλωσης συμμόρφωσης ΕΕ και της τεχνικής τεκμηρίωσης όλων των σχετικών πληροφοριών από τον κατασκευαστή ή τον πάροχο προϊόντων και υπηρεσιών ΤΠΕ·

ιγ-β[...]) τη μέγιστη περίοδο ισχύος των πιστοποιητικών·

ιγ-γ[...]) την πολιτική κοινοποίησης για πιστοποιητικά που έχουν χορηγηθεί, τροποποιηθεί ή ανακληθεί·

ιγ-δ[...]) τις προϋποθέσεις για την αμοιβαία αναγνώριση συστημάτων πιστοποίησης με τρίτες χώρες·

ιγ-ε[...]) κατά περίπτωση, τους κανόνες σχετικά με τον μηχανισμό αξιολόγησης από ομοτίμους όσον αφορά τους οργανισμούς που εκδίδουν ευρωπαϊκά πιστοποιητικά ασφάλειας στον κυβερνοχώρο για υψηλό επίπεδο διασφάλισης [...] δυνάμει του άρθρου 48 παράγραφος 4α.

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 **ή η δήλωση συμμόρφωσης ΕΕ** 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 47α

Αυτοαξιολόγηση της συμμόρφωσης

1. Ένα ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο μπορεί να επιτρέπει τη διενέργεια αξιολόγησης της συμμόρφωσης υπό την αποκλειστική ευθύνη του κατασκευαστή ή του παρόχου προϊόντων και υπηρεσιών ΤΠΕ. Η εν λόγω αξιολόγηση της συμμόρφωσης εφαρμόζεται μόνο σε προϊόντα και υπηρεσίες ΤΠΕ χαμηλού κινδύνου που αντιστοιχεί σε βασικό επίπεδο διασφάλισης.

2. Ο κατασκευαστής ή ο πάροχος προϊόντων και υπηρεσιών ΤΠΕ μπορεί να εκδώσει δήλωση συμμόρφωσης ΕΕ στην οποία να αναφέρεται ότι έχει καταδειχθεί η εκπλήρωση των απαιτήσεων που ορίζονται στο σύστημα. Με την κατάρτιση της εν λόγω δήλωσης, ο κατασκευαστής ή ο πάροχος προϊόντων και υπηρεσιών ΤΠΕ αναλαμβάνει την ευθύνη για τη συμμόρφωση του προϊόντος ή της υπηρεσίας ΤΠΕ με τις απαιτήσεις που ορίζονται στο σύστημα.

3. Ο κατασκευαστής ή ο πάροχος προϊόντων και υπηρεσιών ΤΠΕ τηρεί τη δήλωση συμμόρφωσης ΕΕ και την τεχνική τεκμηρίωση όλων των σχετικών πληροφοριών που αφορούν τη συμμόρφωση των προϊόντων ή υπηρεσιών ΤΠΕ με σύστημα στη διάθεση της εθνικής αρχής πιστοποίησης της ασφάλειας στον κυβερνοχώρο που αναφέρεται στο άρθρο 50 παράγραφος 1 για περίοδο που καθορίζεται στο αντίστοιχο ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο. Αντίγραφο της δήλωσης συμμόρφωσης ΕΕ υποβάλλεται στην εθνική αρχή πιστοποίησης της ασφάλειας στον κυβερνοχώρο και στον ENISA.

4. Η έκδοση δήλωσης της συμμόρφωσης ΕΕ είναι εθελοντική, εκτός αν άλλως ορίζεται στη νομοθεσία της Ένωσης ή στη νομοθεσία των κρατών μελών.

5. Η δήλωση συμμόρφωσης ΕΕ που εκδίδεται δυνάμει του παρόντος άρθρου αναγνωρίζεται σε όλα τα κράτη μέλη.

Άρθρο 48

Πιστοποίηση της ασφάλειας στον κυβερνοχώρο

1. Οι **διαδικασίες**, 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 **ή στη νομοθεσία των κρατών μελών**.

3. Ένα ευρωπαϊκό πιστοποιητικό ασφάλειας στον κυβερνοχώρο δυνάμει του παρόντος άρθρου **που αναφέρεται σε βασικό ή σημαντικό επίπεδο διασφάλισης** εκδίδεται από τους οργανισμούς αξιολόγησης της συμμόρφωσης που αναφέρονται στο άρθρο 51 βάσει κριτηρίων που περιλαμβάνονται στο ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο, που θεσπίζεται 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 [...] οργανισμός μπορεί να είναι:

α) μια εθνική [...] αρχή πιστοποίησης της **ασφάλειας στον κυβερνοχώρο** όπως αναφέρεται στο άρθρο 50 παράγραφος 1·

β) ένας **δημόσιος** οργανισμός που λαμβάνει διαπίστευση ως οργανισμός αξιολόγησης της συμμόρφωσης δυνάμει του άρθρου 51 παράγραφος 1 [...]·

γ) [...].

4α. Σε περιπτώσεις κατά τις οποίες ένα ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο δυνάμει του άρθρου 44 απαιτεί υψηλό επίπεδο διασφάλισης, το πιστοποιητικό μπορεί να εκδοθεί μόνον από εθνική αρχή πιστοποίησης της ασφάλειας στον κυβερνοχώρο που αναφέρεται στο άρθρο 50 παράγραφος 1 ή, βάσει των ακόλουθων προϋποθέσεων, από οργανισμό αξιολόγησης της συμμόρφωσης που αναφέρεται στο άρθρο 51:

α) κατόπιν προηγούμενης έγκρισης από εθνική αρχή πιστοποίησης της ασφάλειας στον κυβερνοχώρο για κάθε ατομικό πιστοποιητικό που εκδίδεται από οργανισμό αξιολόγησης της συμμόρφωσης· ή

β) κατόπιν προηγούμενης γενικής ανάθεσης αυτού του καθήκοντος σε οργανισμό αξιολόγησης της συμμόρφωσης από την εθνική αρχή πιστοποίησης της ασφάλειας στον κυβερνοχώρο.

5. Το φυσικό ή νομικό πρόσωπο που υποβάλλει τις **διαδικασίες,** τα προϊόντα ή τις υπηρεσίες ΤΠΕ του στον μηχανισμό πιστοποίησης [...]**θέτει στη διάθεση** του οργανισμού αξιολόγησης της συμμόρφωσης που αναφέρεται στο άρθρο 51 **ή στην εθνική αρχή πιστοποίησης της ασφάλειας στον κυβερνοχώρο που αναφέρεται στο άρθρο 50, σε περίπτωση που η αρχή αυτή είναι ο οργανισμός που εκδίδει το πιστοποιητικό,** [...] όλες τις πληροφορίες που απαιτούνται για τη διενέργεια της διαδικασίας πιστοποίησης.

5α. Ο κάτοχος πιστοποιητικού ενημερώνει τον οργανισμό που εκδίδει το πιστοποιητικό για τυχόν τρωτά σημεία ή παρατυπίες που εντοπίστηκαν σε μεταγενέστερο στάδιο σχετικά με την ασφάλεια των πιστοποιημένων διαδικασιών, προϊόντων ή υπηρεσιών ΤΠΕ και μπορεί να έχουν αντίκτυπο στις απαιτήσεις σχετικά με την πιστοποίηση. Ο οργανισμός διαβιβάζει τις πληροφορίες αυτές χωρίς αδικαιολόγητη καθυστέρηση στην εθνική αρχή πιστοποίησης της ασφάλειας στον κυβερνοχώρο.

6. Τα πιστοποιητικά εκδίδονται για [...] **την περίοδο που ορίζεται από το εκάστοτε σύστημα πιστοποίησης** και μπορούν να ανανεώνονται, [...] 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 τις **διαδικασίες,** 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 εθνικά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο και οι σχετικές διαδικασίες για τις **διαδικασίες,** 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 τις **διαδικασίες,** 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 **και καλύπτονται από ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο** παραμένουν σε ισχύ έως την ημερομηνία λήξης τους.

Άρθρο 50

Εθνικές* αρχές *πιστοποίησης [...] της ασφάλειας στον κυβερνοχώρο

1. Κάθε κράτος μέλος [...]**ορίζει μία ή περισσότερες** εθνικές [...] **αρχές** πιστοποίησης **της ασφάλειας στον κυβερνοχώρο στο έδαφός του, ή κατόπιν αμοιβαίας συμφωνίας με άλλο κράτος μέλος, ορίζει μία ή περισσότερες αρχές που είναι εγκατεστημένες σε αυτό το άλλο κράτος μέλος προκειμένου να είναι αρμόδιες για τα εποπτικά καθήκοντα στο κράτος μέλος που τις όρισε**.

2. Κάθε κράτος μέλος ενημερώνει την Επιτροπή για την ταυτότητα των **[...] οριζόμενων αρχών και για τα καθήκοντα που τους ανατίθενται**.

3. **Με την επιφύλαξη του άρθρου 48 παράγραφος 4 στοιχείο α) και του άρθρου 48 παράγραφος 4α,** [...] **οι** εθνικές αρχές πιστοποίησης της **ασφάλειας στον κυβερνοχώρο** [...] είναι ανεξάρτητες, σε επίπεδο οργάνωσης, αποφάσεων χρηματοδότησης, νομικής διάρθρωσης και λήψης αποφάσεων, από τις οντότητες τις οποίες επιβλέπουν.

3α. Τα κράτη μέλη διασφαλίζουν ότι οι δραστηριότητες της εθνικής αρχής πιστοποίησης της ασφάλειας στον κυβερνοχώρο που σχετίζονται με την έκδοση πιστοποιητικών σύμφωνα με το άρθρο 48 παράγραφος 4 στοιχείο α) και το άρθρο 48 παράγραφος 4α τηρούν αυστηρό διαχωρισμό των ρόλων και των αρμοδιοτήτων σε σχέση με τις εποπτικές δραστηριότητες του παρόντος άρθρου και ότι αμφότερες οι δραστηριότητες λειτουργούν ανεξάρτητα μεταξύ τους.

4. Τα κράτη μέλη μεριμνούν ώστε οι εθνικές [...] αρχές πιστοποίησης **της ασφάλειας στον κυβερνοχώρο** 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 [...] αρχές πιστοποίησης **της ασφάλειας στον κυβερνοχώρο**:

α) [...]

αα) παρακολουθούν και εφαρμόζουν τις υποχρεώσεις των κατασκευαστών ή των παρόχων προϊόντων και υπηρεσιών ΤΠΕ που είναι εγκατεστημένοι στα αντίστοιχα εδάφη τους όπως ορίζονται στο άρθρο 47α παράγραφοι 2 και 3 και στο αντίστοιχο ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο·

β) [...] **με την επιφύλαξη του άρθρου 51 παράγραφος 1β, παρέχουν βοήθεια στους εθνικούς οργανισμούς διαπίστευσης για την παρακολούθηση και την εποπτεία των** δραστηριοτήτων των οργανισμών αξιολόγησης της συμμόρφωσης για τους σκοπούς του παρόντος κανονισμού [...]·

βα) παρακολουθούν και εποπτεύουν τις δραστηριότητες των οργανισμών που αναφέρονται στο άρθρο 48 παράγραφος 4·

ββ) εξουσιοδοτούν τους οργανισμούς αξιολόγησης της συμμόρφωσης που αναφέρονται στο άρθρο 51 παράγραφος 1β και περιορίζουν, αναστέλλουν ή ανακαλούν υπάρχουσα αδειοδότηση σε περιπτώσεις μη συμμόρφωσης με τις απαιτήσεις του παρόντος κανονισμού·

γ) διεκπεραιώνουν καταγγελίες τις οποίες υποβάλλουν φυσικά ή νομικά πρόσωπα σε σχέση με πιστοποιητικά που έχουν εκδοθεί από [...] **την εθνική αρχή πιστοποίησης της ασφάλειας στον κυβερνοχώρο ή, σύμφωνα με το άρθρο 48 παράγραφος 4α**, **από οργανισμούς αξιολόγησης της συμμόρφωσης**, 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 [...] αρχές πιστοποίησης **της ασφάλειας στον κυβερνοχώρο** ή άλλες δημόσιες αρχές, μεταξύ άλλων μέσω της ανταλλαγής πληροφοριών σχετικά με πιθανή μη συμμόρφωση **διαδικασιών,** 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 [...] αρχές πιστοποίησης **της ασφάλειας στον κυβερνοχώρο** έχουν κατ' ελάχιστον τις ακόλουθες εξουσίες:

α) να ζητούν από τους οργανισμούς αξιολόγησης της συμμόρφωσης**,** [...] τους κατόχους ευρωπαϊκού πιστοποιητικού ασφάλειας στον κυβερνοχώρο **και τους εκδότες δήλωσης συμμόρφωσης ΕΕ** να προσκομίσουν τις πληροφορίες που απαιτούνται για την άσκηση των καθηκόντων τους·

β) να διενεργούν έρευνες, υπό μορφή ελέγχων, των οργανισμών αξιολόγησης της συμμόρφωσης**,** [...] των κατόχων ευρωπαϊκού πιστοποιητικού ασφάλειας στον κυβερνοχώρο **και των εκδοτών δήλωσης συμμόρφωσης ΕΕ**, 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**,** [...] των κατόχων πιστοποιητικού **και των εκδοτών δήλωσης συμμόρφωσης ΕΕ** 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 έχουν εκδοθεί από εθνική αρχή πιστοποίησης της ασφάλειας στον κυβερνοχώρο ή, σύμφωνα με το άρθρο 48 παράγραφος 4α, από οργανισμούς αξιολόγησης της συμμόρφωσης,** τα οποία 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 [...] αρχές πιστοποίησης **της ασφάλειας στον κυβερνοχώρο** 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 διαδικασιών,** 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.

1α. Σε περιπτώσεις κατά τις οποίες εκδίδεται ευρωπαϊκό πιστοποιητικό ασφάλειας στον κυβερνοχώρο από εθνική αρχή πιστοποίησης της ασφάλειας στον κυβερνοχώρο δυνάμει του άρθρου 48 παράγραφος 4 στοιχείο α) και του άρθρου 48 παράγραφος 4α, ο οργανισμός πιστοποίησης της εθνικής αρχής πιστοποίησης της ασφάλειας στον κυβερνοχώρο λαμβάνει διαπίστευση ως οργανισμός αξιολόγησης της συμμόρφωσης δυνάμει της παραγράφου 1 του παρόντος άρθρου.

1β. Κατά περίπτωση, οι οργανισμοί αξιολόγησης της συμμόρφωσης εξουσιοδοτούνται από την εθνική αρχή πιστοποίησης της ασφάλειας στον κυβερνοχώρο να εκτελούν τα καθήκοντά της όταν πληρούν ειδικές ή πρόσθετες απαιτήσεις που ορίζονται στο ευρωπαϊκό σύστημα πιστοποίησης δυνάμει του άρθρου 47 παράγραφος 1 στοιχείο γα).

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 **λαμβάνουν όλα τα ενδεδειγμένα μέτρα εντός εύλογου χρονικού πλαισίου προκειμένου να περιορίσουν, να αναστείλουν ή** να ανακαλέσουν 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 [...] αρχές πιστοποίησης **της ασφάλειας στον κυβερνοχώρο** κοινοποιούν στην Επιτροπή τους [...] οργανισμούς αξιολόγησης της συμμόρφωσης που είναι διαπιστευμένοι **και, κατά περίπτωση, εξουσιοδοτημένοι δυνάμει του άρθρου 51 παράγραφος 1β** 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 [...] αρχή πιστοποίησης **της ασφάλειας στον κυβερνοχώρο** μπορεί να υποβάλει στην Επιτροπή αίτημα διαγραφής οργανισμού αξιολόγησης της συμμόρφωσης, που κοινοποιήθηκε από το συγκεκριμένο κράτος μέλος, 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 [...] αρχή πιστοποίησης **της ασφάλειας στον κυβερνοχώρο**.

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 **εκπροσώπους των** εθνικών [...] αρχών πιστοποίησης **της ασφάλειας στον κυβερνοχώρο ή εκπροσώπους άλλων σχετικών εθνικών αρχών**. [...]**Κάθε μέλος της Ομάδας μπορεί να εκπροσωπεί μόνον ένα άλλο κράτος μέλος**.

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·

βα) να εκδίδει γνώμη σχετικά με το υποψήφιο σύστημα δυνάμει του άρθρου 44 του παρόντος κανονισμού·

γ) να [...] **υποβάλει αίτημα** στον Οργανισμό προκειμένου να προχωρήσει στην επεξεργασία υποψήφιου ευρωπαϊκού συστήματος πιστοποίησης της ασφάλειας στον κυβερνοχώρο σύμφωνα με το άρθρο 44 του παρόντος κανονισμού·

γα) να καταρτίζει και να εγκρίνει κατευθυντήριες γραμμές σχετικά με τα κριτήρια για την αξιολόγηση των προτάσεων που αφορούν την επεξεργασία υποψήφιου συστήματος και υποβάλλονται στην [...] Ομάδα δυνάμει του άρθρου 44 παράγραφος 1α·

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 [...] αρχών πιστοποίησης **της ασφάλειας στον κυβερνοχώρο** βάσει του παρόντος τίτλου μέσω της **ανάπτυξης ικανοτήτων,** της ανταλλαγής πληροφοριών, καθιερώνοντας, ειδικότερα, μεθόδους για την αποτελεσματική ανταλλαγή πληροφοριών σχετικά με όλα τα θέματα που αφορούν την πιστοποίηση της ασφάλειας στον κυβερνοχώρο·

στ-α) να παρέχει υποστήριξη για την εφαρμογή του μηχανισμού αξιολόγησης από ομοτίμους σύμφωνα με τους κανόνες που καθορίζονται σε ευρωπαϊκό σύστημα πιστοποίησης της ασφάλειας στον κυβερνοχώρο δυνάμει του άρθρου 47 παράγραφος 1 στοιχείο ιγ-δ) του παρόντος κανονισμού.

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

Άρθρο 53α

***Δικαίωμα υποβολής καταγγελίας σε εθνική [...] αρχή πιστοποίησης* της ασφάλειας στον κυβερνοχώρο**

1. Τα φυσικά ή νομικά πρόσωπα έχουν το δικαίωμα να υποβάλουν καταγγελία σε εθνική αρχή πιστοποίησης της ασφάλειας στον κυβερνοχώρο σε σχέση με πιστοποιητικό που έχει εκδοθεί από την ίδια αρχή ή, σύμφωνα με το άρθρο 48 παράγραφος 4α, από οργανισμούς αξιολόγησης της συμμόρφωσης.

2. Η εθνική αρχή πιστοποίησης της ασφάλειας στον κυβερνοχώρο στην οποία έχει υποβληθεί καταγγελία ενημερώνει τον καταγγέλλοντα για την πρόοδο και για την έκβαση της καταγγελίας, καθώς και για τη δυνατότητα άσκησης δικαστικής προσφυγής σύμφωνα με το άρθρο 53β.

Άρθρο 53β

Δικαίωμα πραγματικής δικαστικής προσφυγής

1. Τα φυσικά ή νομικά πρόσωπα έχουν το δικαίωμα πραγματικής δικαστικής προσφυγής κατά νομικά δεσμευτικής απόφασης που λαμβάνεται από εθνική αρχή πιστοποίησης της ασφάλειας στον κυβερνοχώρο και αφορά τα εν λόγω πρόσωπα.

2. Τα φυσικά ή νομικά πρόσωπα έχουν το δικαίωμα πραγματικής δικαστικής προσφυγής σε περιπτώσεις κατά τις οποίες η εθνική αρχή πιστοποίησης της ασφάλειας στον κυβερνοχώρο δεν εξετάζει καταγγελία.

3. Οι διαδικασίες κατά εθνικής αρχής πιστοποίησης της ασφάλειας στον κυβερνοχώρο παραπέμπονται στα δικαστήρια του κράτους μέλους στο οποίο είναι εγκατεστημένη η αρχή.

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 5 **παράγραφος 4 στοιχείο β)** 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 III 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

Έναρξη ισχύος

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

1α. Ο παρών κανονισμός εφαρμόζεται από […] εκτός από τα άρθρα 50, 51, 52, 53α, 53β και 54 τα οποία εφαρμόζονται από [24 μήνες μετά την ημερομηνία δημοσίευσής 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*

ΑΠΑΙΤΗΣΕΙΣ ΠΟΥ ΠΡΕΠΕΙ ΝΑ ΠΛΗΡΟΥΝΤΑΙ ΑΠΟ ΤΟΥΣ ΟΡΓΑΝΙΣΜΟΥΣ ΑΞΙΟΛΟΓΗΣΗΣ ΤΗΣ ΣΥΜΜΟΡΦΩΣΗΣ

Οι οργανισμοί αξιολόγησης της συμμόρφωσης που επιθυμούν να αποκτήσουν διαπίστευση πληρούν τις ακόλουθες απαιτήσεις:

1. Ο οργανισμός αξιολόγησης της συμμόρφωσης συστήνεται βάσει της εθνικής νομοθεσίας και διαθέτει νομική προσωπικότητα.

2. Ο οργανισμός αξιολόγησης της συμμόρφωσης είναι τρίτος φορέας, ανεξάρτητος από τον οργανισμό ή το προϊόν ή υπηρεσίες ΤΠΕ που αξιολογεί.

3. Ένας οργανισμός που ανήκει σε ένωση επιχειρήσεων ή επαγγελματική ομοσπονδία που εκπροσωπεί επιχειρήσεις οι οποίες συμμετέχουν στον σχεδιασμό, την κατασκευή, την παροχή, τη συναρμολόγηση, τη χρήση ή τη συντήρηση προϊόντων ή υπηρεσιών ΤΠΕ που αξιολογεί, μπορεί να θεωρείται οργανισμός αξιολόγησης της συμμόρφωσης, υπό την προϋπόθεση ότι η ανεξαρτησία του και η απουσία σύγκρουσης συμφερόντων είναι αποδεδειγμένες.

4. Οι οργανισμοί αξιολόγησης της συμμόρφωσης, τα διευθυντικά τους στελέχη και το προσωπικό που είναι αρμόδιο για την εκτέλεση των καθηκόντων αξιολόγησης της συμμόρφωσης δεν είναι ο σχεδιαστής, ο κατασκευαστής, ο προμηθευτής, ο εγκαταστάτης, ο αγοραστής, ο ιδιοκτήτης, ο χρήστης ή ο συντηρητής του προϊόντος ή υπηρεσίας ΤΠΕ που αξιολογείται, ούτε ο εξουσιοδοτημένος αντιπρόσωπος των ανωτέρω. Τούτο δεν αποκλείει τη χρήση αξιολογημένων προϊόντων που είναι αναγκαία για τις λειτουργίες του οργανισμού αξιολόγησης της συμμόρφωσης ή τη χρήση των προϊόντων αυτών για προσωπικούς σκοπούς.

5. Ο οργανισμός αξιολόγησης της συμμόρφωσης, τα διευθυντικά του στελέχη και το προσωπικό που είναι αρμόδιο για την εκτέλεση των καθηκόντων αξιολόγησης της συμμόρφωσης, δεν εμπλέκονται άμεσα στο σχεδιασμό, την παραγωγή ή την κατασκευή, την εμπορία, την εγκατάσταση, τη χρήση ή τη συντήρηση των εν λόγω προϊόντων ή υπηρεσιών ΤΠΕ, ούτε εκπροσωπούν μέρη που εμπλέκονται στις δραστηριότητες αυτές. Δεν αναλαμβάνουν καμιά δραστηριότητα που μπορεί να έλθει σε σύγκρουση με την ανεξάρτητη κρίση ή την ακεραιότητά τους σε σχέση με δραστηριότητες αξιολόγησης της συμμόρφωσης για τις οποίες είναι κοινοποιημένοι. Τούτο ισχύει ιδίως για συμβουλευτικές υπηρεσίες.

6. Οι οργανισμοί αξιολόγησης της συμμόρφωσης εξασφαλίζουν ότι οι δραστηριότητες των θυγατρικών ή των υπεργολάβων τους δεν επηρεάζουν την εμπιστευτικότητα, την αντικειμενικότητα και την αμεροληψία των οικείων δραστηριοτήτων αξιολόγησης της συμμόρφωσης.

7. Οι οργανισμοί αξιολόγησης της συμμόρφωσης και το προσωπικό τους εκτελούν τις δραστηριότητες αξιολόγησης της συμμόρφωσης με τη μεγαλύτερη επαγγελματική ακεραιότητα και την απαιτούμενη τεχνική επάρκεια στο συγκεκριμένο πεδίο και είναι απαλλαγμένοι από κάθε πίεση και προτροπή, περιλαμβανόμενης της οικονομικής, που θα ήταν δυνατόν να επηρεάσει την κρίση τους ή τα αποτελέσματα των οικείων δραστηριοτήτων αξιολόγησης της συμμόρφωσης, ιδιαίτερα από πρόσωπα ή ομάδες προσώπων που έχουν συμφέρον από τα αποτελέσματα αυτών των δραστηριοτήτων.

8. Ο οργανισμός αξιολόγησης της συμμόρφωσης είναι σε θέση να εκτελεί όλα τα καθήκοντα σχετικά με την αξιολόγηση της συμμόρφωσης που του ανατίθενται από τον παρόντα κανονισμό, είτε πρόκειται για καθήκοντα που εκτελούνται από τον ίδιο τον οργανισμό αξιολόγησης της συμμόρφωσης ή εξ ονόματός του και υπό την ευθύνη του.

9. Ανά πάσα στιγμή και για κάθε διαδικασία αξιολόγησης της συμμόρφωσης και κάθε είδος, κατηγορία ή υποκατηγορία προϊόντων ή υπηρεσιών ΤΠΕ, ο οργανισμός αξιολόγησης της συμμόρφωσης έχει στη διάθεσή του τα εξής απαραίτητα:

α) προσωπικό με τεχνικές γνώσεις και επαρκή και κατάλληλη πείρα για την εκτέλεση των καθηκόντων αξιολόγησης της συμμόρφωσης·

β) περιγραφές ή διαδικασίες σύμφωνα με τις οποίες διενεργείται αξιολόγηση της συμμόρφωσης, εξασφαλίζοντας τη διαφάνεια αυτών των διαδικασιών και τη δυνατότητα αναπαραγωγής τους. Διαθέτει κατάλληλες πολιτικές και διαδικασίες που διακρίνουν μεταξύ καθηκόντων τα οποία εκτελεί ως κοινοποιημένος οργανισμός και άλλων δραστηριοτήτων·

γ) διαδικασίες για την άσκηση δραστηριοτήτων που λαμβάνουν υπόψη το μέγεθος μιας επιχείρησης, τον κλάδο στον οποίο δραστηριοποιείται, τη δομή της, τον βαθμό πολυπλοκότητας της εν λόγω τεχνολογίας του προϊόντος ή υπηρεσίας ΤΠΕ και τον μαζικό ή εν σειρά χαρακτήρα της παραγωγικής διαδικασίας.

10. Ο οργανισμός αξιολόγησης της συμμόρφωσης διαθέτει τα αναγκαία μέσα για την εκτέλεση των τεχνικών και διοικητικών καθηκόντων που συνδέονται κατάλληλα με τις δραστηριότητες αξιολόγησης της συμμόρφωσης, ενώ έχει πρόσβαση σε όλο τον αναγκαίο εξοπλισμό ή εγκαταστάσεις.

11. Το προσωπικό που είναι αρμόδιο για τη διεξαγωγή των δραστηριοτήτων αξιολόγησης της συμμόρφωσης διαθέτει τα ακόλουθα:

α) σε βάθος τεχνική και επαγγελματική κατάρτιση που καλύπτει όλες τις δραστηριότητες αξιολόγησης της συμμόρφωσης·

β) επαρκή γνώση των απαιτήσεων των αξιολογήσεων που διενεργεί και επαρκές κύρος για την εκτέλεση των εν λόγω αξιολογήσεων·

γ) κατάλληλες γνώσεις και κατανόηση των ισχυουσών απαιτήσεων και των προτύπων δοκιμών·

δ) την ικανότητα να καταρτίζει πιστοποιητικά, πρακτικά και εκθέσεις που αποδεικνύουν τη διεξαγωγή των αξιολογήσεων.

12. Εξασφαλίζεται η αμεροληψία των οργανισμών αξιολόγησης της συμμόρφωσης, των διευθυντικών στελεχών τους και του προσωπικού αξιολόγησης.

13. Η αμοιβή των διευθυντικών στελεχών και του προσωπικού του οργανισμού αξιολόγησης της συμμόρφωσης δεν εξαρτάται από τον αριθμό των διεξαγόμενων αξιολογήσεων ή από τα αποτελέσματα των αξιολογήσεων αυτών.

14. Οι οργανισμοί αξιολόγησης της συμμόρφωσης συνάπτουν ασφάλεια αστικής ευθύνης, εφόσον η ευθύνη αυτή δεν έχει αναληφθεί από το κράτος σύμφωνα με το εθνικό δίκαιο, ή εάν το ίδιο το κράτος μέλος φέρει άμεση ευθύνη για την αξιολόγηση της συμμόρφωσης.

15. Το προσωπικό ενός οργανισμού αξιολόγησης της συμμόρφωσης τηρεί το επαγγελματικό απόρρητο για κάθε πληροφορία που περιέρχεται σε γνώση του κατά την εκτέλεση των καθηκόντων του σύμφωνα με την παρούσα οδηγία ή οποιαδήποτε εκτελεστική διάταξη του εθνικού δικαίου, εξαιρουμένης της σχέσης με τις αρμόδιες αρχές του κράτους μέλους στο οποίο διεξάγονται οι δραστηριότητες του οργανισμού.

16. Οι οργανισμοί αξιολόγησης της συμμόρφωσης πληρούν τις απαιτήσεις **του σχετικού** προτύπου **που είναι εναρμονισμένο σύμφωνα με τον κανονισμό (ΕΚ) αριθ. 765/2008 για τη διαπίστευση των οργανισμών αξιολόγησης της συμμόρφωσης που διενεργούν την πιστοποίηση διαδικασιών, προϊόντων ή υπηρεσιών**[...].

17. Οι οργανισμοί αξιολόγησης της συμμόρφωσης εξασφαλίζουν ότι τα εργαστήρια δοκιμών που χρησιμοποιούνται για σκοπούς αξιολόγησης της συμμόρφωσης πληρούν τις απαιτήσεις **του σχετικού** προτύπου **που είναι εναρμονισμένο σύμφωνα με τον κανονισμό (ΕΚ) αριθ. 765/2008 για τη διαπίστευση των εργαστηρίων που πραγματοποιούν δοκιμές** [...].