ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2019/881 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

της 17ης Απριλίου 2019

σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια)

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

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

Έχοντας υπόψη την πρόταση της Ευρωπαϊκής Επιτροπής,

Κατόπιν διαβίβασης του σχεδίου νομοθετικής πράξης στα εθνικά κοινοβούλια,

Έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής [1],

Έχοντας υπόψη τη γνώμη της Επιτροπής των Περιφερειών [2],

Αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία [3],

Εκτιμώντας τα ακόλουθα:

(1) Τα συστήματα δικτύου και πληροφοριών και τα δίκτυα και οι υπηρεσίες ηλεκτρονικών επικοινωνιών διαδραματίζουν ζωτικό ρόλο στην κοινωνία και αποτελούν κεντρικό πυλώνα της οικονομικής ανάπτυξης. Η τεχνολογία πληροφοριών και επικοινωνιών (ΤΠΕ) ενισχύει τα σύνθετα συστήματα που στηρίζουν τις καθημερινές 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, τους οργανισμούς και τις επιχειρήσεις 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 (IoT), ένας εξαιρετικά μεγάλος αριθμός συνδεδεμένων ψηφιακών συσκευών αναμένεται να χρησιμοποιούνται στην Ένωση 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 κυβερνοασφάλειά τους. Στο πλαίσιο αυτό, η περιορισμένη χρήση της πιστοποίησης οδηγεί στο να έχουν οι μεμονωμένοι χρήστες και οι χρήστες από οργανισμούς και επιχειρήσεις ανεπαρκείς πληροφορίες σχετικά με τα χαρακτηριστικά κυβερνοασφάλειας των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ και των διαδικασιών ΤΠΕ, με αποτέλεσμα την υπονόμευση της εμπιστοσύνης στις ψηφιακές λύσεις. Τα συστήματα δικτύου και πληροφοριών έχουν τη δυνατότητα να υποστηρίζουν όλες τις πτυχές της ζωής μας και αποτελούν κινητήρια δύναμη της οικονομικής ανάπτυξης της Ένωσης. Είναι η βάση για την επίτευξη της ψηφιακής ενιαίας αγοράς.

(3) Η αυξημένη ψηφιοποίηση και συνδεσιμότητα οδηγούν σε αυξημένους κινδύνους για την κυβερνοασφάλεια, με αποτέλεσμα να καθίσταται η κοινωνία εν γένει πιο ευάλωτη σε κυβερνοαπειλές και να οξύνονται οι κίνδυνοι που αντιμετωπίζουν τα φυσικά πρόσωπα, συμπεριλαμβανομένων των ευάλωτων προσώπων όπως τα παιδιά. Προκειμένου να μετριαστούν οι εν λόγω κίνδυνοι, είναι ανάγκη να αναληφθούν όλες οι απαραίτητες ενέργειες για τη βελτίωση της κυβερνοασφάλειας στην Ένωση με σκοπό τα συστήματα δικτύου και πληροφοριών, τα δίκτυα επικοινωνιών, τα ψηφιακά προϊόντα, υπηρεσίες και συσκευές που χρησιμοποιούν οι πολίτες, οι οργανισμοί και οι επιχειρήσεις – από τις μικρές και μεσαίες επιχειρήσεις (ΜΜΕ), όπως ορίζονται στη σύσταση 2003/361/ΕΚ της Επιτροπής [4], ως τους διαχειριστές υποδομών ζωτικής σημασίας – να προστατεύονται καλύτερα από τις κυβερνοαπειλές.

[1] ΕΕ C 227 της 28.6.2018, σ. 86.
[2] ΕΕ C 176 της 23.5.2018, σ. 29.
[3] Θέση του Ευρωπαϊκού Κοινοβουλίου της 12ης Μαρτίου 2019 (δεν έχει ακόμα δημοσιευτεί στην Επίσημη Εφημερίδα) και απόφαση του Συμβουλίου της 9ης Απριλίου 2019.
[4] Σύσταση της Επιτροπής, της 6ης Μαΐου 2003, σχετικά με τον ορισμό των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων (ΕΕ L 124 της 20.5.2003, σ. 36).

(4) Διαθέτοντας τις σχετικές πληροφορίες στο ευρύ κοινό, ο Οργανισμός της Ευρωπαϊκής Ένωσης για την κυβερνοασφάλεια (ENISA), όπως ιδρύθηκε με τον κανονισμό (ΕΕ) αριθ. 526/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([5]), συμβάλλει στην ανάπτυξη του κλάδου κυβερνοασφάλειας στην Ένωση, ιδίως για τις ΜΜΕ και τις νεοφυείς επιχειρήσεις. Ο ENISA θα πρέπει να επιδιώξει στενότερη συνεργασία με πανεπιστήμια και ερευνητικούς οργανισμούς ώστε να συμβάλει στη μείωση των εξαρτήσεων από προϊόντα και υπηρεσίες της κυβερνοασφάλειας από χώρες εκτός της Ένωσης και να ενισχύσει τις αλυσίδες εφοδιασμού εντός της Ένωσης.

(5) Οι κυβερνοεπιθέσεις παρουσιάζουν αύξηση και μια συνδεδεμένη οικονομία και κοινωνία που είναι πιο ευάλωτη σε κυβερνοαπειλές και κυβερνοεπιθέσεις χρειάζεται ισχυρότερη άμυνα. Ωστόσο, αν και οι κυβερνοεπιθέσεις είναι συνήθως διασυνοριακές, οι αρμοδιότητες των αρχών για την κυβερνοασφάλεια και των αρχών επιβολής του νόμου, καθώς και τα πολιτικά μέτρα που λαμβάνουν οι εν λόγω αρχές, έχουν κυρίως εθνικό χαρακτήρα. Τα μεγάλης κλίμακας συμβάντα θα μπορούσαν να διαταράξουν την παροχή βασικών υπηρεσιών σε όλη την Ένωση. Τούτο απαιτεί αποτελεσματική και συντονισμένη απόκριση και διαχείριση κρίσεων σε επίπεδο Ένωσης, με βάση ειδικές πολιτικές και ευρύτερα μέσα διασφάλισης της Ευρωπαϊκής αλληλεγγύης και αμοιβαίας συνδρομής. Επιπλέον, η τακτική εκτίμηση της κατάστασης της κυβερνοασφάλειας και της ανθεκτικότητας στην Ένωση με βάση αξιόπιστα ενωσιακά δεδομένα, καθώς και η συστηματική πρόβλεψη των μελλοντικών εξελίξεων, προκλήσεων και απειλών, σε ενωσιακό και σε παγκόσμιο επίπεδο, είναι σημαντικές για τους υπευθύνους χάραξης πολιτικής, τη βιομηχανία και τους χρήστες.

(6) Ενόψει των αυξημένων προκλήσεων που αντιμετωπίζει η Ένωση στον τομέα της κυβερνοασφάλειας, υπάρχει ανάγκη για ολοκληρωμένη σειρά μέτρων που βασίζονται σε προηγούμενες δράσεις της Ένωσης και ευνοούν τους αλληλοενισχυόμενους στόχους. Οι στόχοι αυτοί περιλαμβάνουν την περαιτέρω αύξηση των ικανοτήτων και της ετοιμότητας των κρατών μελών και των επιχειρήσεων, καθώς και τη βελτίωση της συνεργασίας, της ανταλλαγής πληροφοριών και του συντονισμού στα κράτη μέλη και στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης. Επιπλέον, δεδομένης της διασυνοριακής φύσης των κυβερνοαπειλών, υπάρχει ανάγκη αύξησης των ικανοτήτων σε επίπεδο Ένωσης που θα μπορούσαν να συμπληρώσουν τη δράση των κρατών μελών, ιδίως σε περιπτώσεις μεγάλης κλίμακας διασυνοριακών συμβάντων και κρίσεων, λαμβάνοντας ταυτόχρονα υπόψη τη σημασία της διατήρησης και περαιτέρω ενίσχυσης των εθνικών ικανοτήτων αντιμετώπισης κυβερνοαπειλών σε κάθε κλίμακα.

(7) Απαιτούνται επίσης επιπλέον προσπάθειες για την αύξηση της ευαισθητοποίησης των πολιτών, των οργανισμών και των επιχειρήσεων σε ζητήματα κυβερνοασφάλειας. Επιπλέον, δεδομένου ότι τα συμβάντα υπονομεύουν την εμπιστοσύνη στους παρόχους ψηφιακών υπηρεσιών και στην ίδια την ψηφιακή ενιαία αγορά, ιδίως μεταξύ των καταναλωτών, η εμπιστοσύνη θα πρέπει να ενισχυθεί περαιτέρω με την παροχή πληροφοριών με διαφάνεια σχετικά με το επίπεδο ασφάλειας των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ και των διαδικασιών ΤΠΕ που υπογραμμίζουν ότι ακόμη και ένα υψηλό επίπεδο πιστοποίησης κυβερνοασφάλειας δεν μπορεί να εγγυηθεί απολύτως την ασφάλεια των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ και των διαδικασιών ΤΠΕ. Στην αύξηση της εμπιστοσύνης μπορεί να συμβάλει η πιστοποίηση σε επίπεδο Ένωσης, με την παροχή κοινών απαιτήσεων κυβερνοασφάλειας και κριτηρίων αξιολόγησης για όλες τις εθνικές αγορές και τους τομείς.

(8) Η κυβερνοασφάλεια δεν είναι μόνο ζήτημα τεχνολογίας, αλλά ζήτημα όπου σημαντικό ρόλο κατέχει η ανθρώπινη συμπεριφορά. Ως εκ τούτου, θα πρέπει να ενθαρρυνθεί η «κυβερνοϋγιεινή», δηλαδή απλά μέτρα ρουτίνας τα οποία, όταν εφαρμόζονται και εκτελούνται τακτικά από πολίτες, οργανισμούς και επιχειρήσεις, ελαχιστοποιούν την έκθεσή τους σε κινδύνους από κυβερνοαπειλές.

(9) Για να ενισχυθούν οι ενωσιακές δομές κυβερνοασφάλειας, είναι σημαντικό να διατηρηθούν και να αναπτυχθούν οι ικανότητες των κρατών μελών για την ολοκληρωμένη αντιμετώπιση των κυβερνοαπειλών, συμπεριλαμβανομένων των διασυνοριακών συμβάντων.

(10) Οι επιχειρήσεις και οι μεμονωμένοι καταναλωτές θα πρέπει να έχουν ακριβείς πληροφορίες σχετικά με το επίπεδο διασφάλισης στο οποίο έχει πιστοποιηθεί η ασφάλεια των οικείων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ. Ταυτόχρονα, κανένα προϊόν ΤΠΕ ή υπηρεσία ΤΠΕ δεν είναι πλήρως κυβερνοασφαλές και πρέπει να προωθηθούν και να έχουν προτεραιότητα οι βασικοί κανόνες της κυβερνοϋγιεινής. Λόγω της αυξανόμενης προσφοράς συσκευών του IoT, υπάρχει μια σειρά μέτρων τα οποία ο ιδιωτικός τομέας μπορεί να λάβει σε εθελοντική βάση για να ενισχύσει την εμπιστοσύνη στην ασφάλεια των προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ.

(11) Τα σύγχρονα προϊόντα και συστήματα ΤΠΕ συχνά ενσωματώνουν και βασίζονται σε μία ή περισσότερες τεχνολογίες και συνιστώσες τρίτων όπως ενότητες λογισμικού, βιβλιοθήκες ή διεπαφές προγραμματισμού εφαρμογών. Αυτή η σχέση, που καλείται «εξάρτηση», θα μπορούσε να δημιουργήσει πρόσθετους κινδύνους για την κυβερνοασφάλεια, καθώς τα τρωτά σημεία που βρίσκονται σε συνιστώσες τρίτων θα μπορούσαν επίσης να επηρεάσουν την ασφάλεια των προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ. Σε πολλές περιπτώσεις, ο προσδιορισμός και η τεκμηρίωση τέτοιων εξαρτήσεων παρέχει τη δυνατότητα στους τελικούς χρήστες των προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ να βελτιώσουν τις ενέργειές τους για τη διαχείριση κινδύνων που συνδέονται με την κυβερνοασφάλεια, βελτιώνοντας, για παράδειγμα, τις διαδικασίες που χρησιμοποιούν οι χρήστες για τη διαχείριση και διόρθωση των τρωτών σημείων της κυβερνοασφάλειας.

([5]) 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).

(12) Οι οργανισμοί, οι κατασκευαστές ή οι πάροχοι υπηρεσιών που εμπλέκονται στον σχεδιασμό και στην ανάπτυξη προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ θα πρέπει να ενθαρρύνονται να εφαρμόζουν μέτρα, κατά τα πρώτα στάδια του σχεδιασμού και της ανάπτυξης, ώστε η ασφάλεια των εν λόγω προϊόντων, υπηρεσιών και διαδικασιών να προστατεύεται στον μέγιστο δυνατό βαθμό, κατά τρόπο που να θεωρείται δεδομένο ότι θα γίνουν κυβερνοεπιθέσεις και οι επιπτώσεις τους να προβλέπονται και να ελαχιστοποιούνται («ασφάλεια βάσει σχεδιασμού» - «security-by-design»). Μέριμνα για την ασφάλεια θα πρέπει να διασφαλίζεται καθ' όλη τη διάρκεια ζωής του προϊόντος ΤΠΕ, της υπηρεσίας ΤΠΕ ή της διαδικασίας ΤΠΕ με συνεχή εξέλιξη των διαδικασιών σχεδιασμού και ανάπτυξης, ώστε να μειώνεται ο κίνδυνος βλάβης λόγω κακόβουλης εκμετάλλευσης.

(13) Οι επιχειρήσεις, οι οργανισμοί και ο δημόσιος τομέας θα πρέπει να διαμορφώνουν τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ ή τις διαδικασίες ΤΠΕ που σχεδιάζουν κατά τρόπο που να διασφαλίζει υψηλότερο επίπεδο ασφάλειας το οποίο επιτρέπει στον πρώτο χρήστη να λαμβάνει μια προεπιλεγμένη ρύθμιση με τις πλέον ασφαλείς παραμέτρους («ασφάλεια εξ ορισμού»), μειώνοντας κατ' αυτόν τον τρόπο την επιβάρυνση των χρηστών με την ανάγκη κατάλληλης ρύθμισης προϊόντος ΤΠΕ, υπηρεσίας ΤΠΕ ή διαδικασίας ΤΠΕ. Η ασφάλεια εξ ορισμού δεν θα πρέπει να απαιτεί εκτενή ρύθμιση ή ειδικές τεχνικές γνώσεις ή μη διαισθητική συμπεριφορά εκ μέρους του χρήστη και θα πρέπει να λειτουργεί εύκολα και αξιόπιστα όταν εφαρμόζεται. Εάν, κατά περίπτωση, η ανάλυση κινδύνου και χρηστικότητας καταλήξει στο συμπέρασμα ότι μια τέτοια προεπιλεγμένη ρύθμιση δεν είναι εφικτή, οι χρήστες θα πρέπει να παροτρύνονται να επιλέξουν την πιο ασφαλή ρύθμιση.

(14) Με τον κανονισμό (ΕΚ) αριθ. 460/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([6]) δημιουργήθηκε ο ENISA με σκοπό να συμβάλλει στην επίτευξη των στόχων της διασφάλισης υψηλού και αποτελεσματικού 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. Ο κανονισμός (ΕΚ) αριθ. 1007/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([7]) παρέτεινε τη θητεία του ENISA έως τον Μάρτιο του 2012. Ο κανονισμός (ΕΕ) αριθ. 580/2011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([8]) παρέτεινε περαιτέρω τη θητεία του ENISA έως τις 13 Σεπτεμβρίου 2013. Ο κανονισμός (ΕΕ) αριθ. 526/2013 παρέτεινε τη θητεία του ENISA έως τις 19 Ιουνίου 2020.

(15) Η Ένωση έχει λάβει ήδη σημαντικά μέτρα για τη διασφάλιση της κυβερνοασφάλειας και την ενίσχυση της εμπιστοσύνης στις ψηφιακές τεχνολογίες. Το 2013 θεσπίστηκε η Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο με σκοπό τον προσανατολισμό των μέτρων πολιτικής της Ένωσης έναντι των κυβερνοαπειλών και των κυβερνοκινδύνων. Στο πλαίσιο της προσπάθειας της να προστατέψει καλύτερα τους πολίτες που είναι συνδεδεμένοι επιγραμμικά, η πρώτη νομική πράξη της Ένωσης στον τομέα της κυβερνοασφάλειας εκδόθηκε το 2016 υπό τη μορφή της οδηγίας (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([9]). Η οδηγία (ΕΕ) 2016/1148 θέσπισε απαιτήσεις σχετικά με τις ικανότητες σε εθνικό επίπεδο στον τομέα της κυβερνοασφάλειας και τους πρώτους μηχανισμούς ενίσχυσης της στρατηγικής και επιχειρησιακής συνεργασίας μεταξύ των κρατών μελών και εισήγαγε 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 προμήθειας και διανομής πόσιμου νερού, 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 στη στήριξη της εφαρμογής της εν λόγω οδηγίας. Επιπλέον, σημαντική προτεραιότητα του ευρωπαϊκού θεματολογίου για την ασφάλεια είναι η αποτελεσματική καταπολέμηση του κυβερνοεγκλήματος, συμβάλλοντας έτσι στον συνολικό στόχο της επίτευξης υψηλού επιπέδου κυβερνοασφάλειας. Άλλες νομικές πράξεις όπως ο κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([10]) και οι οδηγίες του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου 2002/58/ΕΚ ([11]) και (ΕΕ) 2018/1972 ([12]) επίσης συμβάλλουν σε ένα υψηλό επίπεδο κυβερνοασφάλειας στην ψηφιακή ενιαία αγορά.

([6]) 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).

([7]) 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).

([8]) 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).

([9]) Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (ΕΕ L 194 της 19.7.2016, σ. 1).

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

([11]) Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) (ΕΕ L 201 της 31.7.2002, σ. 37).

([12]) Οδηγία (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2018, για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών (ΕΕ L 321 της 17.12.2018, σ. 36).

(16) Από τη θέσπιση της Στρατηγικής της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο το 2013 και την τελευταία επανεξέταση της εντολής του ENISA, το συνολικό πολιτικό πλαίσιο έχει αλλάξει σημαντικά καθώς το παγκόσμιο περιβάλλον έχει γίνει πιο αβέβαιο και λιγότερο ασφαλές. Υπό αυτές τις συνθήκες και σε συνάρτηση με τη θετική εξέλιξη του ρόλου του ENISA που αποτελεί σημείο αναφοράς για συμβουλές και εμπειρογνωσία και διευκολύνει τη συνεργασία και τη δημιουργία ικανοτήτων καθώς και στο πλαίσιο της νέας πολιτικής της Ένωσης για την κυβερνοασφάλεια, είναι απαραίτητο να επανεξεταστεί η εντολή του ENISA, να καθοριστεί ο ρόλος του στο οικοσύστημα της κυβερνοασφάλειας που έχει μεταβληθεί και να διασφαλιστεί η αποτελεσματική συμβολή του στην αντιμετώπιση από την Ένωση των προκλήσεων στον τομέα της κυβερνοασφάλειας που απορρέουν από τη ριζική μεταβολή της φύσης των κυβερνοαπειλών, οι οποίες, όπως αναγνωρίστηκε στο πλαίσιο της αξιολόγησης του ENISA, δεν αντιμετωπίζονται επαρκώς από την παρούσα εντολή.

(17) Ο ENISA που ιδρύεται με τον παρόντα κανονισμό θα πρέπει να αποτελεί συνέχεια του ENISA όπως συστάθηκε δυνάμει του κανονισμού (ΕΕ) αριθ. 526/2013. Ο ENISA θα πρέπει να εκτελεί τα καθήκοντα που του ανατίθενται με τον παρόντα κανονισμό και άλλες νομικές πράξεις της Ένωσης στον τομέα της κυβερνοασφάλειας, μεταξύ άλλων, με την παροχή συμβουλών και εμπειρογνωμοσύνης 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 συμφεροντούχων του ιδιωτικού τομέα, να υποβάλλει προτάσεις πολιτικής στην Επιτροπή και τα κράτη μέλη, να λειτουργεί ως σημείο αναφοράς για τομεακές πρωτοβουλίες πολιτικής της Ένωσης όσον αφορά ζητήματα κυβερνοασφάλειας και να ενθαρρύνει την επιχειρησιακή συνεργασία μεταξύ των κρατών μελών και μεταξύ των κρατών μελών και των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης.

(18) Στο πλαίσιο της απόφασης 2004/97/ΕΚ, Ευρατόμ την οποία έλαβαν με κοινή συμφωνία οι αντιπρόσωποι των κρατών μελών, συνερχόμενοι σε επίπεδο αρχηγού κράτους ή κυβερνήσεως ([13]), 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 ENISA θα πρέπει να διασφαλίζει τις βέλτιστες δυνατές συνθήκες για την εύρυθμη και αποδοτική λειτουργία του ENISA. 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 ENISA 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 ENISA. Οι απαιτούμενες διευθετήσεις θα πρέπει να θεσπισθούν με συμφωνία μεταξύ του ENISA και του κράτους μέλους υποδοχής, με προηγούμενη έγκριση του διοικητικού συμβουλίου του ENISA.

(19) Δεδομένων των αυξανόμενων κινδύνων και προκλήσεων που αντιμετωπίζει η Ένωση στον τομέα της κυβερνοασφάλειας, θα πρέπει να αυξηθούν οι χρηματοδοτικοί και οι ανθρώπινοι πόροι του ENISA, κατ' αντιστοιχία προς τον ενισχυμένο ρόλο και τα αυξημένα καθήκοντά του και την καθοριστική του θέση στο οικοσύστημα των οργανισμών που προασπίζονται το ψηφιακό οικοσύστημα της Ένωσης, επιτρέποντας στον ENISA να εκπληρώσει αποτελεσματικά τα καθήκοντα που του ανατίθενται βάσει του παρόντος κανονισμού.

(20) Ο ENISA 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 ENISA θα πρέπει να στηρίζει ενεργά 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, αποφεύγοντας τυχόν αλληλεπικάλυψη εργασιών και προωθώντας τις συνέργειες. Επιπροσθέτως, ο ENISA θα πρέπει να αξιοποιεί τις εισροές από τον ιδιωτικό τομέα και άλλους σχετικούς συμφεροντούχους, καθώς και τη συνεργασία με αυτούς. Με μια σειρά καθηκόντων θα πρέπει να καθοριστεί ο τρόπος με τον οποίο ο ENISA οφείλει να επιτύχει τους στόχους του, ενώ θα πρέπει να καθίσταται δυνατή η ευελιξία στο έργο του.

(21) Για να είναι σε θέση να παράσχει επαρκή υποστήριξη στην επιχειρησιακή συνεργασία μεταξύ των κρατών μελών, ο ENISA θα πρέπει να ενισχύσει περαιτέρω τις τεχνικές και ανθρώπινες ικανότητες και δεξιότητές του. Ο ENISA θα πρέπει να αυξήσει την τεχνογνωσία και τις ικανότητές του. Ο ENISA και τα κράτη μέλη, σε εθελοντική βάση, θα μπορούσαν να αναπτύξουν προγράμματα για την απόσπαση εθνικών εμπειρογνωμόνων στον ENISA, τη δημιουργία ομάδων εμπειρογνωμόνων και την ανταλλαγή προσωπικού.

(22) Ο ENISA θα πρέπει να επικουρεί την Επιτροπή μέσω συμβουλών, γνωμοδοτήσεων και αναλύσεων σχετικά με θέματα της Ένωσης που αφορούν τη χάραξη, τις επικαιροποιήσεις και τις αναθεωρήσεις της πολιτικής και του δικαίου στο πεδίο της κυβερνοασφάλειας και τις ειδικές ανά τομέα πτυχές αυτού του πεδίου προκειμένου να ενισχύσει τη σημασία της πολιτικής και της νομοθεσίας της Ένωσης που σχετίζονται με την κυβερνοασφάλεια και να επιτρέψει τη συνεπή εφαρμογή της εν λόγω πολιτικής και νομοθεσίας σε εθνικό επίπεδο. Ο ENISA θα πρέπει να ενεργεί ως σημείο αναφοράς για τις συμβουλές και την εμπειρογνωσία για τομεακές πρωτοβουλίες πολιτικής και νομοθεσίας της Ένωσης σε περιπτώσεις που αφορούν ζητήματα κυβερνοασφάλειας. Ο ENISA θα πρέπει να ενημερώνει τακτικά το Ευρωπαϊκό Κοινοβούλιο για τις δραστηριότητές του.

([13]) Απόφαση 2004/97/ΕΚ, Ευρατόμ την οποία έλαβαν με κοινή συμφωνία οι αντιπρόσωποι των κρατών μελών, συνερχόμενοι σε επίπεδο αρχηγού κράτους ή κυβερνήσεως, της 13ης Δεκεμβρίου 2003, σχετικά με τον καθορισμό της έδρας ορισμένων οργανισμών της Ευρωπαϊκής Ένωσης (ΕΕ L 29 της 3.2.2004, σ. 15).

(23) Ο δημόσιος πυρήνας του ανοιχτού διαδικτύου, δηλαδή τα κύρια πρωτόκολλα και οι υποδομές του που είναι παγκόσμιο δημόσιο αγαθό, παρέχει τη βασική λειτουργικότητα του διαδικτύου στο σύνολό του και στηρίζει την κανονική του λειτουργία. Ο ENISA θα πρέπει να στηρίζει την ασφάλεια του δημόσιου πυρήνα του ανοιχτού διαδικτύου και τη σταθερότητα της λειτουργίας του, συμπεριλαμβανομένων, χωρίς να περιορίζεται σε αυτά, των βασικών πρωτοκόλλων (ιδίως DNS, BGP και IPv6), τη λειτουργίας του συστήματος ονομάτων τομέα (χώρου) (όπως της λειτουργίας όλων των τομέων ανωτάτου επιπέδου) και τη λειτουργίας της βασικής ζώνης.

(24) Το βασικό καθήκον του ENISA είναι η προώθηση της συνεπούς εφαρμογής του σχετικού νομικού πλαισίου, ειδικότερα δε η αποτελεσματική εφαρμογή της οδηγίας (ΕΕ) 2016/1148 και άλλων συναφών νομικών εργαλείων που περιέχουν πτυχές της κυβερνοασφάλειας, που είναι απαραίτητη για την αύξηση της κυβερνοανθεκτικότητας. Υπό το πρίσμα του ταχέως εξελισσόμενου τοπίου των κυβερνοαπειλών, είναι σαφές ότι οφείλεται να παρέχεται στήριξη στα κράτη μέλη μέσω μιας πιο συνεκτικής διατομεακής προσέγγισης στην οικοδόμηση κυβερνοανθεκτικότητας.

(25) Ο ENISA 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 κυβερνοαπειλών και συμβάντων και σε σχέση με την ασφάλεια συστημάτων δικτύου και πληροφοριών. Συγκεκριμένα, ο ENISA θα πρέπει να υποστηρίζει την ανάπτυξη και την ενίσχυση εθνικών και ενωσιακών ομάδων παρέμβασης για συμβάντα που αφορούν την ασφάλεια των υπολογιστών («CSIRT») που προβλέπονται στην οδηγία (ΕΕ) 2016/1148, με σκοπό την επίτευξη υψηλού κοινού επιπέδου ωριμότητάς τους στην Ένωση. Οι δραστηριότητες που διεξάγει ο ENISA σχετικά με τις επιχειρησιακές ικανότητες των κρατών μελών θα πρέπει να υποστηρίζουν ενεργά τις δράσεις που αναλαμβάνουν τα κράτη μέλη για να εκπληρώνουν τις υποχρεώσεις τους που απορρέουν από την οδηγία (ΕΕ) 2016/1148 και συνεπώς δεν θα πρέπει να τις υπερσκελίζουν.

(26) Ο ENISA θα πρέπει επίσης να συμβάλλει στην ανάπτυξη και την επικαιροποίηση των στρατηγικών σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών σε επίπεδο Ένωσης και, κατόπιν αιτήματος, σε επίπεδο κρατών μελών, ιδίως όσον αφορά την κυβερνοασφάλεια, και να προωθεί τη διάδοση των εν λόγω στρατηγικών και να παρακολουθεί την πρόοδο της υλοποίησής τους. Ο ENISA θα πρέπει επίσης να συμβάλλει στην κάλυψη των αναγκών κατάρτισης και εκπαιδευτικού υλικού, μεταξύ άλλων των αναγκών των δημόσιων φορέων, και, όπου είναι σκόπιμο, σε μεγάλο βαθμό, να «εκπαιδεύει τους εκπαιδευτικούς», με βάση το πλαίσιο ψηφιακών ικανοτήτων για τους πολίτες και με σκοπό την παροχή συνδρομής στα κράτη μέλη και στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης για την ανάπτυξη των δικών τους ικανοτήτων κατάρτισης.

(27) Ο ENISA θα πρέπει να στηρίζει τα κράτη μέλη στον τομέα της ευαισθητοποίησης και της εκπαίδευσης για την κυβερνοασφάλεια διευκολύνοντας τον στενότερο συντονισμό και την ανταλλαγή βέλτιστων πρακτικών μεταξύ των κρατών μελών. Η υποστήριξη αυτή θα μπορούσε να συνίσταται στην ανάπτυξη ενός δικτύου εθνικών εκπαιδευτικών σημείων επαφής και στην ανάπτυξη μιας πλατφόρμας κατάρτισης για την κυβερνοασφάλεια. Το δίκτυο των εθνικών εκπαιδευτικών σημείων επαφής θα μπορούσε να λειτουργήσει στο πλαίσιο του δικτύου εθνικών υπαλλήλων-συνδέσμων και να αποτελέσει αφετηρία για τον μελλοντικό συντονισμό εντός των κρατών μελών.

(28) Ο ENISA θα πρέπει να επικουρεί την ομάδα συνεργασίας που θεσπίστηκε με την οδηγία (ΕΕ) 2016/1148 στην εκτέλεση των καθηκόντων της, συγκεκριμένα μέσω της παροχής εμπειρογνωμοσύνης, συμβουλών και της διευκόλυνσης της ανταλλαγής βέλτιστων πρακτικών, μεταξύ άλλων όσον αφορά τον προσδιορισμό φορέων εκμετάλλευσης βασικών υπηρεσιών από τα κράτη μέλη, καθώς και όσον αφορά διασυνοριακές εξαρτήσεις σε σχέση με κινδύνους και συμβάντα.

(29) Με στόχο να δοθούν κίνητρα για τη συνεργασία δημόσιου και ιδιωτικού τομέα και εντός του ιδιωτικού τομέα και ειδικότερα με σκοπό τη στήριξη της προστασίας των υποδομών ζωτικής σημασίας, ο ENISA 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 οποίον θα αντιμετωπίζονται κανονιστικά ζητήματα που σχετίζονται με την ανταλλαγή πληροφοριών, για παράδειγμα μέσω της διευκόλυνσης της θέσπισης τομεακών κέντρων κοινοχρησίας και ανάλυσης πληροφοριών.

(30) Καθώς οι πιθανές αρνητικές επιπτώσεις των τρωτών σημείων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ αυξάνονται συνεχώς, ο εντοπισμός και η διόρθωση αυτών των τρωτών σημείων παίζουν σημαντικό ρόλο στη μείωση του συνολικού κινδύνου για την κυβερνοασφάλεια. Η συνεργασία μεταξύ οργανισμών, κατασκευαστών ή παρόχων τρωτών προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ, καθώς και μελών της ερευνητικής κοινότητας για την κυβερνοασφάλεια και των κυβερνήσεων που εντοπίζουν τρωτά σημεία έχει αποδειχθεί ότι αυξάνει σημαντικά τόσο τα ποσοστά εντοπισμού όσο και τη διόρθωση των τρωτών σημείων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ. Συντονισμένη δημοσιοποίηση τρωτών σημείων σημαίνει μια διαρθρωμένη διαδικασία συνεργασίας στην οποία τα τρωτά σημεία αναφέρονται στον ιδιοκτήτη του συστήματος πληροφοριών, παρέχοντας στον οργανισμό την ευκαιρία να διαγνώσει και να διορθώσει το τρωτό σημείο πριν να αποκαλυφθούν σε τρίτα μέρη ή στο ευρύ κοινό λεπτομερείς πληροφορίες σχετικά με τα τρωτά σημεία. Η διαδικασία προβλέπει επίσης τον συντονισμό μεταξύ του «εντοπιστή» και του οργανισμού όσον αφορά τη δημοσιοποίηση των εν λόγω τρωτών σημείων. Οι πολιτικές της συντονισμένης δημοσιοποίησης τρωτών σημείων θα μπορούσαν να διαδραματίσουν σημαντικό ρόλο στις προσπάθειες των κρατών μελών για την ενίσχυση της κυβερνοασφάλειας.

(31) Ο ENISA θα πρέπει να συγκεντρώνει και να αναλύει εθνικές εκθέσεις από τις CSIRT και τη διοργανική ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική για τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης που θεσπίστηκε με τον διακανονισμό μεταξύ του Ευρωπαϊκού Κοινοβουλίου, του Ευρωπαϊκού Συμβουλίου, του Συμβουλίου της Ευρωπαϊκής Ένωσης, της Ευρωπαϊκής Επιτροπής, του Δικαστηρίου της Ευρωπαϊκής Ένωσης, της Ευρωπαϊκής Κεντρικής Τράπεζας, του Ευρωπαϊκού Ελεγκτικού Συνεδρίου, της Ευρωπαϊκής Υπηρεσίας Εξωτερικής Δράσης, της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής, της Ευρωπαϊκής Επιτροπής των Περιφερειών και της Ευρωπαϊκής Τράπεζας Επενδύσεων σχετικά με την οργάνωση και τη λειτουργία ομάδας αντιμετώπισης έκτακτων αναγκών στην πληροφορική για τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης (CERT-ΕΕ) ([14]) οι οποίες ανταλλάσσονται σε εθελοντική βάση με σκοπό τη συμβολή στον καθορισμό κοινών διαδικασιών, γλώσσας και ορολογίας για την ανταλλαγή πληροφοριών. Υπό αυτές τις συνθήκες ο ENISA θα πρέπει να εξασφαλίζει τη συμμετοχή του ιδιωτικού τομέα στο πλαίσιο της οδηγίας (ΕΕ) 2016/1148 που καθορίζει τους λόγους εθελούσιας ανταλλαγής τεχνικών πληροφοριών σε επιχειρησιακό επίπεδο εντός του δικτύου ομάδων απόκρισης συμβάντων που αφορούν την ασφάλεια των υπολογιστών («δίκτυο CSIRT») που δημιουργήθηκε με την εν λόγω οδηγία.

(32) Ο ENISA θα πρέπει να συμβάλλει στην αντιμετώπιση σε επίπεδο Ένωσης σε περίπτωση μεγάλης κλίμακας διασυνοριακών συμβάντων και κρίσεων που αφορούν την κυβερνοασφάλεια. Το εν λόγω καθήκον θα πρέπει να εκτελείται σύμφωνα με την εντολή του ENISA όπως αυτή καθορίζεται από τον παρόντα κανονισμό και με βάση μια προσέγγιση που θα αποφασιστεί από τα κράτη μέλη στο πλαίσιο της σύστασης (ΕΕ) 2017/1584 της Επιτροπής ([15]) και των συμπερασμάτων του Συμβουλίου της 26ης Ιουνίου 2018 για τη συντονισμένη αντιμετώπιση σε επίπεδο ΕΕ συμβάντων και κρίσεων ασφάλειας μεγάλης κλίμακας στον κυβερνοχώρο. Το εν λόγω καθήκον 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 έχουν την ευθύνη διαχείρισης κρίσεων. Επιπλέον, ο ENISA θα πρέπει να στηρίζει την επιχειρησιακή συνεργασία μεταξύ των κρατών μελών, όταν ζητείται από ένα ή περισσότερα κράτη μέλη, στον χειρισμό συμβάντων από τεχνικής άποψης, μέσω της διευκόλυνσης της σχετικής ανταλλαγής τεχνικών λύσεων μεταξύ των κρατών μελών και μέσω της παροχής εισροών σε δημόσιες επικοινωνίες. Ο ENISA θα πρέπει να στηρίζει την επιχειρησιακή συνεργασία δοκιμάζοντας τις ρυθμίσεις μιας τέτοιας συνεργασίας μέσω τακτικών ασκήσεων κυβερνοασφάλειας.

(33) Για τη στήριξη της επιχειρησιακής συνεργασίας, ο ENISA θα πρέπει να χρησιμοποιεί τη διαθέσιμη τεχνική και επιχειρησιακή εμπειρογνωσία της CERT-EU μέσω διαρθρωμένης συνεργασίας. Η διαρθρωμένη αυτή συνεργασία θα μπορούσε να ενισχύσει την εμπειρογνωσία του ENISA. Όπου συντρέχει περίπτωση, θα πρέπει να θεσπίζονται συγκεκριμένες ρυθμίσεις μεταξύ των δύο οντοτήτων με σκοπό τον καθορισμό της πρακτικής εφαρμογής της εν λόγω συνεργασίας και την αποφυγή της αλληλεπικάλυψης δραστηριοτήτων.

(34) Εκτελώντας το καθήκον του που αφορά τη στήριξη της επιχειρησιακής συνεργασίας στο πλαίσιο του δικτύου των CSIRT, ο ENISA θα πρέπει να μπορεί να παρέχει στήριξη στα κράτη μέλη κατόπιν αιτήματός τους, όπως για παράδειγμα παρέχοντας συμβουλές για το πώς να βελτιώσουν τις ικανότητές τους να προλαμβάνουν, να εντοπίζουν και να αντιμετωπίζουν συμβάντα, διευκολύνοντας τον τεχνικό χειρισμό συμβάντων που έχουν σημαντικό ή ουσιαστικό αντίκτυπο ή διασφαλίζοντας τη διενέργεια αναλύσεων σχετικά με κυβερνοαπειλές και συμβάντα. Ο ENISA θα πρέπει να διευκολύνει τον τεχνικό χειρισμό συμβάντων που έχουν σημαντικό ή ουσιαστικό αντίκτυπο, παρέχοντας ειδικότερα στήριξη στην εθελούσια ανταλλαγή τεχνικών λύσεων μεταξύ των κρατών μελών ή παράγοντας συνδυαστικές τεχνικές πληροφορίες, όπως τεχνικές λύσεις που ανταλλάσσουν σε εθελοντική βάση τα κράτη μέλη. Η σύσταση (ΕΕ) 2017/1584 συνιστά ότι 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 κυβερνοασφάλεια. Τέτοιου είδους πληροφορίες θα βοηθήσουν περαιτέρω τον ENISA στην εκπλήρωση του καθήκοντός του για τη στήριξη της επιχειρησιακής συνεργασίας.

(35) Στο πλαίσιο της τακτικής συνεργασίας σε τεχνικό επίπεδο με σκοπό τη στήριξη της ευαισθητοποίησης ως προς την κατάσταση στην Ένωση, ο ENISA θα πρέπει, σε στενή συνεργασία με τα κράτη μέλη, να εκπονεί τακτική αναλυτική τεχνική έκθεση για την κατάσταση της κυβερνοασφάλειας στην ΕΕ όσον αφορά συμβάντα και κυβερνοαπειλές, με βάση τις πληροφορίες που είναι δημόσια διαθέσιμες, τις αναλύσεις του και εκθέσεις του που έχει μοιραστεί με τις CSIRT των κρατών μελών ή τα εθνικά ενιαία κέντρα επαφής για την ασφάλεια των συστημάτων δικτύου και πληροφοριών («ενιαία κέντρα επαφής») που προβλέπονται στην οδηγία (ΕΕ) 2016/1148, όλα σε εθελοντική βάση, το Ευρωπαϊκό Κέντρο για τα Κυβερνοεγκλήματα (EC3) στη Ευρωπόλ, τη CERT-EU και, όπου συντρέχει περίπτωση, το Κέντρο ανάλυσης πληροφοριών και κατάστασης της Ευρωπαϊκής Ένωσης (EU INTCEN) στην Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης. Η εν λόγω έκθεση θα πρέπει να διατίθεται στο Συμβούλιο, στην Επιτροπή, στον Ύπατο Εκπρόσωπο της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας και στο δίκτυο CSIRT.

(36) Η στήριξη από τον ENISA για τις εκ των υστέρων τεχνικές έρευνες συμβάντων με σημαντικό ή ουσιαστικό αντίκτυπο οι οποίες αναλαμβάνονται κατόπιν αιτήματος των ενδιαφερόμενων κρατών μελών θα πρέπει να επικεντρώνεται στην πρόληψη μελλοντικών συμβάντων. Τα ενδιαφερόμενα κράτη μέλη θα πρέπει να παρέχουν τις απαραίτητες πληροφορίες και συνδρομή προκειμένου να μπορεί ο ENISA να στηρίζει αποτελεσματικά την εκ των υστέρων τεχνική έρευνα.

([14]) ΕΕ C 12 της 13.1.2018, σ. 1.

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

(37) Τα κράτη μέλη μπορούν να καλούν τις επιχειρήσεις τις οποίες αφορά το συμβάν να συνεργάζονται παρέχοντας τις απαραίτητες πληροφορίες και συνδρομή στον ENISA με την επιφύλαξη του δικαιώματός τους να προστατεύουν εμπορικά ευαίσθητες πληροφορίες και πληροφορίες που αφορούν τη δημόσια ασφάλεια.

(38) Για την καλύτερη κατανόηση των προκλήσεων στον τομέα της κυβερνοασφάλειας και με σκοπό την παροχή στρατηγικών μακροπρόθεσμων συμβουλών στα κράτη μέλη και τα θεσμικά όργανα και λοιπά όργανα και οργανισμούς της Ένωσης, ο ENISA πρέπει να αναλύει τους υφιστάμενους και αναδυόμενους κινδύνους για την κυβερνοασφάλεια. Για τον σκοπό αυτό, ο ENISA θα πρέπει, σε συνεργασία με τα κράτη μέλη και, αν κρίνεται σκόπιμο, με τα στατιστικά όργανα και λοιπά όργανα, 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, ιδίως στην κυβερνοασφάλεια. Ο ENISA θα πρέπει επιπλέον να στηρίζει τα κράτη μέλη και τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης κατά τον προσδιορισμό των αναδυόμενων κινδύνων στην κυβερνοασφάλεια και την πρόληψη των συμβάντων, πραγματοποιώντας αναλύσεις των κυβερνοαπειλών, των τρωτών σημείων και των συμβάντων στον κυβερνοχώρο.

(39) Προκειμένου να αυξήσει την ανθεκτικότητα της Ένωσης, ο ENISA θα πρέπει να αναπτύξει εμπειρογνωμοσύνη στον τομέα της κυβερνοασφάλειας των υποδομών, ιδίως για τη στήριξη των τομέων που παρατίθενται στον κατάλογο του παραρτήματος ΙΙ της οδηγίας (ΕΕ) 2016/1148 και εκείνων που χρησιμοποιούνται από τους παρόχους ψηφιακών υπηρεσιών που παρατίθενται στον κατάλογο του παραρτήματος ΙΙΙ της εν λόγω οδηγίας, παρέχοντας συμβουλές, εκδίδοντας κατευθυντήριες γραμμές και ανταλλάσσοντας βέλτιστες πρακτικές. Με στόχο τη διασφάλιση ευκολότερης πρόσβασης σε καλύτερα διαρθρωμένες πληροφορίες σχετικά με τους κινδύνους και τα πιθανά διορθωτικά μέτρα που αφορούν την κυβερνοασφάλεια, ο ENISA θα πρέπει να αναπτύξει και να διατηρεί τον «κόμβο πληροφοριών» της Ένωσης, μια μονοαπευθυντική πύλη που παρέχει στο κοινό πληροφορίες σχετικά με την κυβερνοασφάλεια που δημιουργούνται στην Ένωση και προέρχονται από τα θεσμικά και λοιπά όργανα και οργανισμούς. Η διευκόλυνση της πρόσβασης σε καλύτερα δομημένες πληροφορίες σχετικά με τους κινδύνους για την κυβερνοασφάλεια και τις πιθανές διορθωτικές ενέργειες θα μπορούσε επίσης να βοηθήσει τα κράτη μέλη να ενισχύσουν τις ικανότητές τους και να ευθυγραμμίσουν τις πρακτικές τους, βελτιώνοντας έτσι τη συνολική τους ανθεκτικότητα έναντι των κυβερνοεπιθέσεων.

(40) Ο ENISA θα πρέπει να συμβάλλει στην ευαισθητοποίηση του κοινού όσον αφορά τους κινδύνους κυβερνοασφάλειας, μεταξύ άλλων με πανευρωσιακή εκστρατεία ευαισθητοποίησης προάγοντας την εκπαίδευση, και στην παροχή καθοδήγησης όσον αφορά τις ορθές πρακτικές για μεμονωμένους χρήστες στοχεύοντας σε πολίτες, οργανώσεις και επιχειρήσεις. Ο ENISA θα πρέπει επίσης να συμβάλλει στην προώθηση βέλτιστων πρακτικών και λύσεων, συμπεριλαμβανομένης της κυβερνοϋγιεινής και του κυβερνογραμματισμού, σε επίπεδο πολιτών, οργανώσεων και επιχειρήσεων, συλλέγοντας και αναλύοντας δημόσια διαθέσιμες πληροφορίες σχετικά με σημαντικά συμβάντα και συντάσσοντας και δημοσιεύοντας εκθέσεις και καθοδήγηση για πολίτες, οργανισμούς και επιχειρήσεις, και στη βελτίωση του συνολικού επιπέδου ετοιμότητας και ανθεκτικότητάς τους. Ο ENISA θα πρέπει να προσπαθεί επίσης να παρέχει στους καταναλωτές σχετικές πληροφορίες για τα ισχύοντα συστήματα πιστοποίησης, για παράδειγμα μέσω κατευθυντήριων γραμμών και συστάσεων. Επιπλέον, ο ENISA θα πρέπει να διοργανώνει, σύμφωνα με το σχέδιο δράσης για την ψηφιακή εκπαίδευση που συστάθηκε με την ανακοίνωση της Επιτροπής της 17ης Ιανουαρίου 2018 και 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 τον ψηφιακό γραμματισμό και την ευαισθητοποίηση σχετικά με τις ενδεχόμενες κυβερνοαπειλές, συμπεριλαμβανομένων των επιγραμμικών εγκληματικών δραστηριοτήτων όπως οι επιθέσεις ηλεκτρονικού «ψαρέματος» (phishing), δίκτυα προγραμμάτων ρομπότ (botnet), χρηματοπιστωτική και τραπεζική απάτη και περιστατικά απάτης με δεδομένα, καθώς και την προώθηση βασικών συμβουλών για την πολυπαραγοντική πιστοποίηση γνησιότητας, τη δημιουργία patch ασφαλείας (patching), την κρυπτογράφηση, την ανωνυμοποίηση και την προστασία των δεδομένων.

(41) Ο ENISA θα πρέπει να διαδραματίζει κεντρικό ρόλο στην επιτάχυνση της ευαισθητοποίησης των τελικών χρηστών ως προς την ασφάλεια των συσκευών και την ασφαλή χρήση των υπηρεσιών και θα πρέπει να προάγει σε επίπεδο Ένωσης την ασφάλεια βάσει σχεδιασμού και την προστασία της ιδιωτικής ζωής εκ σχεδιασμού (privacy-by-design). Προς επίτευξη του στόχου αυτού, ο ENISA θα πρέπει να αξιοποιεί τις διαθέσιμες βέλτιστες πρακτικές και εμπειρίες, ιδίως τις βέλτιστες πρακτικές και εμπειρίες ακαδημαϊκών ιδρυμάτων και ερευνητών στον τομέα της ασφάλειας ΤΠ.

(42) Προκειμένου να υποστηρίζει τις επιχειρήσεις που δραστηριοποιούνται στον τομέα της κυβερνοασφάλειας, καθώς και τους χρήστες λύσεων σχετικών με την κυβερνοασφάλεια, ο ENISA θα πρέπει να αναπτύξει και να διατηρεί ένα «παρατηρητήριο αγοράς», διενεργώντας τακτικές αναλύσεις και διαδίδοντας πληροφορίες για τις κύριες τάσεις στην αγορά της κυβερνοασφάλειας, τόσο από την πλευρά της ζήτησης όσο και από την πλευρά της προσφοράς.

(43) Ο ENISA θα πρέπει να συμβάλλει στις προσπάθειες της Ένωσης για συνεργασία με διεθνείς οργανισμούς, καθώς και εντός των συναφών διεθνών πλαισίων συνεργασίας στον τομέα της κυβερνοασφάλειας. Ειδικότερα, ο ENISA θα πρέπει να συμβάλλει, κατά περίπτωση, στη συνεργασία με οργανισμούς όπως ο ΟΟΣΑ, ο ΟΑΣΕ και το ΝΑΤΟ. Η συνεργασία αυτή θα μπορούσε να περιλαμβάνει κοινές ασκήσεις κυβερνοασφάλειας και κοινό συντονισμό της αντιμετώπισης συμβάντων. Οι εν λόγω δραστηριότητες οφείλουν να πραγματοποιούνται με πλήρη σεβασμό των αρχών της συμμετοχικότητας, της αμοιβαιότητας και της αυτονομίας λήψης αποφάσεων της Ένωσης, χωρίς να θίγεται ο ιδιαίτερος χαρακτήρας της πολιτικής ασφάλειας και άμυνας κάθε κράτους μέλους.

(44) Για να διασφαλίσει την πλήρη επιτυχία των στόχων του, ο ENISA θα πρέπει να συνεργάζεται με σχετικές εποπτικές αρχές της Ένωσης και με άλλες αρμόδιες αρχές στην Ένωση, τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης, συμπεριλαμβανομένης της CERT-EU, του EC3, του Ευρωπαϊκού Οργανισμού Άμυνας (ΕΟΑ), του Ευρωπαϊκού Οργανισμού Παγκόσμιου Δορυφορικού Συστήματος Πλοήγησης (Ευρωπαϊκός Οργανισμός GNSS), του Φορέα Ευρωπαϊκών Ρυθμιστικών Αρχών για τις Ηλεκτρονικές Επικοινωνίες (BEREC), του Ευρωπαϊκού Οργανισμού για τη λειτουργική διαχείριση συστημάτων ΤΠ μεγάλης κλίμακας στον χώρο Ελευθερίας, Ασφάλειας και Δικαιοσύνης (eu-LISA), της Ευρωπαϊκής Κεντρικής Τράπεζας (ΕΚΤ), της Ευρωπαϊκής Αρχής Τραπεζών (ΕΑΤ), του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων, του Οργανισμού Συνεργασίας των Ρυθμιστικών Αρχών Ενέργειας (ACER), του Οργανισμού Ασφάλειας της Αεροπορίας της Ευρωπαϊκής Ένωσης (ΕΟΑΑ) και οποιουδήποτε άλλους οργανισμού της Ένωσης που εμπλέκεται στην κυβερνοασφάλεια. Ο ENISA 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 θέματα κυβερνοασφάλειας 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 συμβουλευτική ομάδα του ENISA. Όταν ο ENISA συνεργάζεται με αρχές 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.

(45) Θα μπορούσαν να δημιουργηθούν εταιρικές σχέσεις με ακαδημαϊκά ιδρύματα που αναλαμβάνουν ερευνητικές πρωτοβουλίες στους σχετικούς τομείς και οι πληροφορίες από τις οργανώσεις καταναλωτών και άλλους φορείς θα πρέπει να φτάνουν μέσω κατάλληλων διαύλων και να λαμβάνονται υπόψη.

(46) Ο ENISA, υπό την ιδιότητά του ως Γραμματεία του δικτύου CSIRT, θα πρέπει να στηρίζει τις CSIRT των κρατών μελών και τη CERT-EU στην επιχειρησιακή συνεργασία σχετικά με τα σχετικά καθήκοντα του δικτύου CSIRT, όπως αναφέρεται στην οδηγία (ΕΕ) 2016/1148. Ακόμη, ο ENISA θα πρέπει να προωθεί και να υποστηρίζει τη συνεργασία μεταξύ των οικείων CSIRT σε περίπτωση συμβάντων, επιθέσεων ή διαταραχών στη λειτουργία των δικτύων ή στην υποδομή την οποία διαχειρίζονται ή προστατεύουν οι CSIRT και αφορούν ή μπορούν να αφορούν τουλάχιστον δύο CSIRT, λαμβάνοντας δεόντως υπόψη τις τυποποιημένες επιχειρησιακές διαδικασίες του δικτύου CSIRT.

(47) Προκειμένου να αυξηθεί η ετοιμότητα της Ένωσης στην απόκριση σε συμβάντα, ο ENISA θα πρέπει να διοργανώνει σε τακτική βάση ασκήσεις για την κυβερνοασφάλεια σε επίπεδο Ένωσης και, κατόπιν αιτήματος, να στηρίζει τα κράτη μέλη και τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης στη διοργάνωση τέτοιων ασκήσεων. Ανά διετία θα πρέπει να διοργανώνονται γενικές ασκήσεις μεγάλης κλίμακας οι οποίες περιλαμβάνουν τεχνικά, επιχειρησιακά και στρατηγικά στοιχεία. Επιπλέον, ο ENISA θα πρέπει να μπορεί να διοργανώνει τακτικά λιγότερο εκτενείς ασκήσεις με τον ίδιο στόχο, δηλαδή να αυξηθεί η ετοιμότητα της Ένωσης στην απόκριση σε συμβάντα.

(48) Ο ENISA θα πρέπει να αναπτύσσει περαιτέρω και να διατηρεί την εμπειρογνωσία του στην πιστοποίηση της κυβερνοασφάλειας προκειμένου να υποστηρίζει την ενωσιακή πολιτική στον τομέα αυτό. Ο ENISA θα πρέπει να αξιοποιεί τις υφιστάμενες βέλτιστες πρακτικές και να προάγει την εισαγωγή πιστοποίησης για την κυβερνοασφάλεια εντός της Ένωσης, μεταξύ άλλων συμβάλλοντας στη θέσπιση και τη διατήρηση ενός πλαισίου πιστοποίησης της κυβερνοασφάλειας σε ενωσιακό επίπεδο (ευρωπαϊκό πλαίσιο πιστοποίησης για την κυβερνοασφάλεια), προκειμένου να αυξηθεί η διαφάνεια της εξασφάλισης της κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ, ενισχύοντας κατ' αυτόν τον τρόπο την εμπιστοσύνη στην ψηφιακή εσωτερική αγορά και στην ανταγωνιστικότητά της.

(49) Οι αποδοτικές πολιτικές κυβερνοασφάλειας 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 κυβερνοασφάλειας στην Ένωση. Για τον σκοπό αυτό, ο ENISA θα πρέπει να υποστηρίζει τη συνεργασία μεταξύ των συμφεροντούχων του δημόσιου και του ιδιωτικού τομέα σε επίπεδο Ένωσης και να διευκολύνει 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 δικτύου και πληροφοριών.

(50) Ο ENISA θα πρέπει να παροτρύνει τα κράτη μέλη, τους κατασκευαστές ή τους παρόχους προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ να ανεβάζουν το γενικό επίπεδο των προτύπων ασφάλειας, έτσι ώστε όλοι οι χρήστες του διαδικτύου να μπορούν να λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίζουν την προσωπική τους κυβερνοασφάλεια, και θα πρέπει να παρέχει κίνητρα για να το πράξουν. Πιο συγκεκριμένα, οι κατασκευαστές και οι πάροχοι προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ θα πρέπει να παρέχουν τις τυχόν αναγκαίες ενημερώσεις και να ανακαλούν, να αποσύρουν ή να ανακυκλώνουν προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ ή διαδικασίες ΤΠΕ που δεν πληρούν τα πρότυπα κυβερνοασφάλειας, ενώ οι εισαγωγείς και οι διανομείς θα πρέπει να διασφαλίζουν ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ που διαθέτουν στην αγορά της Ένωσης συμμορφώνονται με τις ισχύουσες απαιτήσεις και δεν παρουσιάζουν κίνδυνο για τους καταναλωτές της Ένωσης.

(51) Σε συνεργασία με τις αρμόδιες αρχές, ο ENISA θα πρέπει να μπορεί να διαδίδει πληροφορίες όσον αφορά το επίπεδο κυβερνοασφάλειας των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ και των διαδικασιών ΤΠΕ που διατίθενται στην εσωτερική αγορά και να εκδίδει προειδοποιήσεις που στοχεύουν τους κατασκευαστές ή τους παρόχους προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ και απαιτούν από αυτούς να βελτιώνουν την ασφάλεια των οικείων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ, συμπεριλαμβανομένης της κυβερνοασφάλειας.

(52) Ο ENISA θα πρέπει να συνυπολογίζει πλήρως τις τρέχουσες δραστηριότητες έρευνας, ανάπτυξης και τεχνολογικής 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 και προτεραιότητες στον τομέα της κυβερνοασφάλειας. Προκειμένου να προσδιορίζονται οι ερευνητικές ανάγκες και προτεραιότητες, ο ENISA θα πρέπει επίσης να συμβουλεύεται τις οικείες ομάδες χρηστών. Ειδικότερα, θα μπορούσε να καθιερωθεί συνεργασία με το Ευρωπαϊκό Συμβούλιο Έρευνας, το Ευρωπαϊκό Ινστιτούτο Καινοτομίας και Τεχνολογίας και το Ινστιτούτο Μελετών της Ευρωπαϊκής Ένωσης για Θέματα Ασφάλειας.

(53) Ο ENISA θα πρέπει να διαβουλεύεται τακτικά με τους οργανισμούς τυποποίησης, ιδίως τους ευρωπαϊκούς, κατά την προετοιμασία των ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας.

(54) Οι κυβερνοαπειλές είναι παγκόσμιο ζήτημα. Υπάρχει ανάγκη στενότερης διεθνούς συνεργασίας για τη βελτίωση των προτύπων κυβερνοασφάλειας, συμπεριλαμβανομένης της ανάγκης ορισμού κοινών προτύπων συμπεριφοράς και υιοθέτησης δεοντολογικών κανόνων, της χρήσης διεθνών προτύπων και της από κοινού χρήσης πληροφοριών, για την προώθηση ταχύτερης διεθνούς συνεργασίας για την αντιμετώπιση θεμάτων ασφάλειας δικτύων και πληροφοριών και για την προώθηση κοινής παγκόσμιας προσέγγισης τέτοιων θεμάτων. Για τον σκοπό αυτό, ο ENISA θα πρέπει να υποστηρίζει την εκτενέστερη ευρωπαϊκή συμμετοχή και τη συνεργασία με τρίτες χώρες και διεθνείς οργανισμούς, παρέχοντας την απαιτούμενη εμπειρογνωμοσύνη και δυνατότητα ανάλυσης στα σχετικά θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης, κατά περίπτωση.

(55) Ο ENISA 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 Ένωσης και εμπίπτουν στην εντολή του ENISA.

(56) Είναι λογικό και ενδεδειγμένο να εφαρμοστούν ορισμένες αρχές σε σχέση με τη διακυβέρνηση του ENISA για τη συμμόρφωση στην κοινή δήλωση και την κοινή προσέγγιση που συμφωνήθηκαν τον Ιούλιο του 2012 στη διοργανική ομάδα εργασίας για τους αποκεντρωμένους οργανισμούς της Ένωσης, η οποία έχει ως αποστολή τον εξορθολογισμό των δραστηριοτήτων των αποκεντρωμένων οργανισμών και τη βελτίωση της απόδοσής τους. Οι συστάσεις στην κοινή δήλωση και στην κοινή προσέγγιση θα πρέπει επίσης να αντικατοπτρίζονται, κατά περίπτωση, στα προγράμματα εργασιών του ENISA, στις αξιολογήσεις του ENISA και στις πρακτικές του ENISA όσον αφορά την υποβολή εκθέσεων και την άσκηση της διοίκησης.

(57) Το διοικητικό συμβούλιο, που απαρτίζεται από εκπροσώπους των κρατών μελών και της Επιτροπής, θα πρέπει να καθορίζει τη γενική κατεύθυνση των εργασιών του ENISA 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 εκτέλεσης του προϋπολογισμού, την έγκριση κατάλληλων δημοσιονομικών κανόνων, τη θέσπιση διαφανών διαδικασιών εργασίας για τη λήψη αποφάσεων από τον ENISA, την έγκριση του ενιαίου εγγράφου προγραμματισμού του ENISA, την έγκριση του εσωτερικού κανονισμού του Οργανισμού, καθώς και τον διορισμό του εκτελεστικού διευθυντή και τη λήψη απόφασης για παράταση και λήξη της θητείας του εκτελεστικού διευθυντή.

(58) Για την ορθή και αποτελεσματική λειτουργία του ENISA, 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. Η Επιτροπή και τα κράτη μέλη θα πρέπει επίσης να καταβάλλουν προσπάθειες για τον περιορισμό της εναλλαγής των αντίστοιχων αντιπροσώπων τους στο διοικητικό συμβούλιο, προκειμένου να εξασφαλίζεται η συνέχεια του έργου του.

(59) Για την ομαλή λειτουργία του ENISA, ο εκτελεστικός διευθυντής του επιβάλλεται να διορίζεται βάσει προσόντων και αποδεδειγμένων διοικητικών και διευθυντικών ικανοτήτων, καθώς και βάσει ικανοτήτων και πείρας στον τομέα της κυβερνοασφάλειας. Τα καθήκοντα του εκτελεστικού διευθυντή θα πρέπει να εκτελούνται με πλήρη ανεξαρτησία. Ο εκτελεστικός διευθυντής θα πρέπει να εκπονεί πρόταση για το ετήσιο πρόγραμμα εργασίας του ENISA, κατόπιν προηγούμενης διαβούλευσης με την Επιτροπή, και να λαμβάνει όλα τα αναγκαία μέτρα για να διασφαλίζει την ορθή εκτέλεση του εν λόγω προγράμματος εργασίας. Ο εκτελεστικός διευθυντής θα πρέπει να καταρτίζει ετήσια έκθεση προς υποβολή στο διοικητικό συμβούλιο η οποία περιλαμβάνει την υλοποίηση του ετήσιου προγράμματος εργασίας του ENISA, να εκπονεί σχέδιο της κατάστασης των εκτιμώμενων εσόδων και εξόδων του ENISA 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, ιδίως θεμάτων επιστημονικής, τεχνικής, νομικής ή κοινωνικοοικονομικής φύσης. Ειδικότερα, όσον αφορά την επεξεργασία συγκεκριμένου υποψήφιου ευρωπαϊκού συστήματος πιστοποίησης της κυβερνοασφάλειας («υποψήφιο σύστημα»), θεωρείται αναγκαία η συγκρότηση ad hoc ομάδας εργασίας. Ο εκτελεστικός διευθυντής θα πρέπει

να διασφαλίζει ότι τα μέλη των ad hoc ομάδων εργασίας επιλέγονται σύμφωνα με τα υψηλότερα πρότυπα εμπειρογνωσίας, με στόχο τη διασφάλιση ισορροπίας όσον αφορά τα δύο φύλα και κατάλληλης ισορροπίας, αναλόγως του συγκεκριμένου θέματος προς συζήτηση, των δημόσιων διοικήσεων των κρατών μελών, των θεσμικών οργάνων και λοιπών οργάνων και οργανισμών 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.

(60) 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 των αποφάσεων του διοικητικού συμβουλίου.

(61) Ο ENISA θα πρέπει να διαθέτει μια συμβουλευτική ομάδα του ENISA ως συμβουλευτικό όργανο, προκειμένου να διασφαλίζει τον τακτικό διάλογο με τον ιδιωτικό τομέα, τις οργανώσεις καταναλωτών και άλλους σχετικούς συμφεροντούχους. Η συμβουλευτική ομάδα του ENISA, η οποία συγκροτείται από το διοικητικό συμβούλιο κατόπιν πρότασης του εκτελεστικού διευθυντή, θα πρέπει να επικεντρώνεται σε θέματα που αφορούν τους συμφεροντούχους και να τα θέτει υπόψη του ENISA. Θα πρέπει να ζητείται η γνώμη της συμβουλευτικής ομάδας του ENISA ιδίως όσον αφορά το σχέδιο ετήσιου προγράμματος εργασίας του ENISA. Η σύνθεση της συμβουλευτικής ομάδας του ENISA και τα καθήκοντα με τα οποία επιφορτίζεται θα πρέπει να διασφαλίζουν επαρκή αντιπροσώπευση των συμφεροντούχων στις εργασίες του ENISA.

(62) Θα πρέπει να συσταθεί ομάδα συμφεροντούχων για την πιστοποίηση της κυβερνοασφάλειας προκειμένου να βοηθήσει τον ENISA και την Επιτροπή διευκολύνοντας τη διαβούλευση σχετικών συμφεροντούχων. Η ομάδα συμφεροντούχων για την πιστοποίηση της κυβερνοασφάλειας θα πρέπει να απαρτίζεται από μέλη που εκπροσωπούν σε ισορροπημένη αναλογία τον κλάδο, τόσο από την πλευρά της ζήτησης όσο και από την πλευρά της προσφοράς προϊόντων ΤΠΕ και υπηρεσιών ΤΠΕ, συμπεριλαμβανομένων ιδίως των ΜΜΕ, των παρόχων ψηφιακών υπηρεσιών, των Ευρωπαϊκών και διεθνών οργανισμών τυποποίησης, των οργανισμών διαπίστευσης, των εποπτικών αρχών προστασίας δεδομένων και των οργανισμών αξιολόγησης της συμμόρφωσης δυνάμει του κανονισμού (ΕΚ) αριθ. 765/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([16]) και της ακαδημαϊκής κοινότητας καθώς και των οργανώσεων καταναλωτών.

(63) Ο ENISA θα πρέπει να θεσπίσει και να εφαρμόζει κανόνες για την πρόληψη και τη διαχείριση συγκρούσεων συμφερόντων. Ο ENISA 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 ([17]). Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα από τον ENISA θα πρέπει να υπόκειται στον κανονισμό (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([18]). Ο ENISA θα πρέπει να συμμορφώνεται με τις διατάξεις που ισχύουν για τα θεσμικά όργανα και λοιπά όργανα και οργανισμούς της Ένωσης, καθώς και με την εθνική νομοθεσία σχετικά με τον χειρισμό πληροφοριών, ιδίως των ευαίσθητων μη διαβαθμισμένων πληροφοριών και των διαβαθμισμένων πληροφοριών της Ευρωπαϊκής Ένωσης (EUCI).

(64) Προκειμένου να διασφαλισθεί η πλήρης αυτονομία και ανεξαρτησία του ENISA και για να είναι σε θέση να ασκήσει πρόσθετα καθήκοντα, ακόμα κι αν αυτά είναι έκτακτα και απρόβλεπτα, θα πρέπει να διατεθεί στον ENISA επαρκής και αυτόνομος προϋπολογισμός του οποίου τα έσοδα θα πρέπει να προέρχονται πρωτίστως από εισφορές της Ένωσης και από εισφορές τρίτων χωρών που συμμετέχουν στις εργασίες του ENISA. Ο κατάλληλος προϋπολογισμός είναι πρωταρχικής σημασίας για να διασφαλιστεί ότι ο ENISA διαθέτει επαρκείς ικανότητες για την εκπλήρωση όλων των αυξανόμενων καθηκόντων του και την επίτευξη των στόχων του. Η πλειονότητα των υπαλλήλων του ENISA θα πρέπει να εμπλέκεται άμεσα στην επιτέλεση των επιχειρησιακών καθηκόντων στο πλαίσιο της εντολής του ENISA. Θα πρέπει να επιτρέπεται στο κράτος μέλος υποδοχής και σε οποιοδήποτε άλλο κράτος μέλος να συνεισφέρει εθελοντικά στον προϋπολογισμό του ENISA. 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 του ENISA για να εξασφαλίζει διαφάνεια και λογοδοσία.

(65) Η πιστοποίηση της κυβερνοασφάλειας παίζει σημαντικό ρόλο στην ενίσχυση της αξιοπιστίας και της ασφάλειας για τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ και τις διαδικασίες ΤΠΕ. Η ψηφιακή ενιαία αγορά, και πιο συγκεκριμένα η οικονομία δεδομένων και το IoT, μπορούν να ευδοκιμήσουν μόνο αν υπάρχει εμπιστοσύνη από το ευρύ κοινό ότι αυτά τα προϊόντα, αυτές οι υπηρεσίες και διαδικασίες παρέχουν ένα ορισμένο επίπεδο κυβερνοασφάλειας. Τα συνδεδεμένα και αυτοματοποιημένα αυτοκίνητα, οι ηλεκτρονικές ιατρικές συσκευές, τα συστήματα ελέγχου βιομηχανικού αυτοματισμού και 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 (ΕΕ) 2016/1148 είναι επίσης τομείς στους οποίους η πιστοποίηση της κυβερνοασφάλειας είναι καίριας σημασίας.

([16]) Κανονισμός (ΕΚ) αριθ. 765/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Ιουλίου 2008, για τον καθορισμό των απαιτήσεων διαπίστευσης και εποπτείας της αγοράς όσον αφορά την εμπορία των προϊόντων και για την κατάργηση του κανονισμού (ΕΟΚ) αριθ. 339/93 του Συμβουλίου (ΕΕ L 218 της 13.8.2008, σ. 30).

([17]) 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).

([18]) Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ (ΕΕ L 295 της 21.11.2018, σ. 39).

(66) 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 κυβερνοασφάλεια. Η προμήθεια προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ εντός της ενιαίας αγοράς παραμένει πολύ κατακερματισμένη γεωγραφικά. Αυτό οφείλεται στο γεγονός ότι ο κλάδος της κυβερνοασφάλειας 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 Ένωσης συμπεριλαμβάνεται στα λοιπά κενά που επηρεάζουν την ενιαία αγορά στον τομέα της κυβερνοασφάλειας. Το γεγονός αυτό καθιστά δύσκολο τον ανταγωνισμό των ευρωπαϊκών επιχειρήσεων σε εθνικό, ενωσιακό και παγκόσμιο επίπεδο. Μειώνει επίσης την επιλογή βιώσιμων και χρήσιμων τεχνολογιών κυβερνοασφάλειας στις οποίες έχουν πρόσβαση άτομα και επιχειρήσεις. Ομοίως, στην ανακοίνωση του 2017 για την Ενδιάμεση επανεξέταση της εφαρμογής της στρατηγικής για την ψηφιακή ενιαία αγορά - Μια συνδεδεμένη ψηφιακή ενιαία αγορά για όλους, 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 εσωτερικής αγοράς.

(67) Επί του παρόντος, η πιστοποίηση της κυβερνοασφάλειας για τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ και τις διαδικασίες 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 πιστοποίησης της κυβερνοασφάλειας δεν αναγνωρίζεται καταρχήν στα άλλα κράτη μέλη. Επομένως, οι εταιρείες ενδέχεται να πρέπει να πιστοποιούν τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ και τις ΤΠΕ διαδικασίες τους στα διάφορα κράτη μέλη όπου δραστηριοποιούνται, για παράδειγμα με σκοπό τη συμμετοχή τους σε εθνικές διαδικασίες προμηθειών, κάτι που συνεπάγεται πρόσθετο κόστος για τις εταιρείες. Επιπλέον, ενώ νέα συστήματα κάνουν την εμφάνισή τους, δεν φαίνεται να υπάρχει συνεκτική και ολιστική προσέγγιση όσον αφορά τα οριζόντια ζητήματα κυβερνοασφάλειας, για παράδειγμα στο πεδίο του IoT. Τα υφιστάμενα συστήματα παρουσιάζουν σοβαρές αδυναμίες και διαφορές ως προς την κάλυψη των προϊόντων, τα επίπεδα διασφάλισης, τα ουσιαστικά κριτήρια και την πραγματική χρήση, εμποδίζοντας τους μηχανισμούς αμοιβαίας αναγνώρισης εντός της Ένωσης.

(68) Έχουν καταβληθεί προσπάθειες προκειμένου να διασφαλιστεί η αμοιβαία αναγνώριση πιστοποιητικών στην Ένωση. 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 ορισμένα μόνο από τα κράτη μέλη. Αυτό το γεγονός περιορίζει την αποτελεσματικότητα της συμφωνίας αμοιβαίας αναγνώρισης της SOG-IS από την άποψη της εσωτερικής αγοράς.

(69) Επομένως, είναι απαραίτητη η έγκριση κοινής προσέγγισης και η θέσπιση ενός ευρωπαϊκού πλαισίου πιστοποίησης της κυβερνοασφάλειας που αφενός θα προβλέπει τις κύριες οριζόντιες απαιτήσεις για τα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας που πρόκειται να αναπτυχθούν και αφετέρου θα καθιστά δυνατή την αναγνώριση των ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας και των δηλώσεων συμμόρφωσης ΕΕ για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ ή διαδικασίες ΤΠΕ και τη χρήση τους σε όλα τα κράτη μέλη. Εν προκειμένω, είναι σημαντικό να αξιοποιηθούν τα υπάρχοντα εθνικά και διεθνή συστήματα, καθώς και τα καθεστώτα αμοιβαίας αναγνώρισης, ιδίως της SOG-IS, και να καταστεί δυνατή η ομαλή μετάβαση από τα υφιστάμενα συστήματα στο πλαίσιο τέτοιων καθεστώτων σε συστήματα σύμφωνα με το νέο ευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας. Το ευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας θα πρέπει να έχει διττό σκοπό. Αφενός θα πρέπει να συμβάλλει στην ενίσχυση της εμπιστοσύνης σε προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ που έχουν λάβει πιστοποίηση βάσει των ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας. Αφετέρου, θα πρέπει να συμβάλλει στην αποφυγή συγκρουόμενων ή αλληλεπικαλυπτόμενων συστημάτων εθνικής πιστοποίησης της κυβερνοασφάλειας και, ως εκ τούτου, να περιορίζει το κόστος για τις επιχειρήσεις που δραστηριοποιούνται στην ψηφιακή ενιαία αγορά. Τα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας δεν θα πρέπει να κάνουν διακρίσεις και θα πρέπει να βασίζονται σε ευρωπαϊκά ή διεθνή πρότυπα, εκτός αν αυτά τα πρότυπα είναι αναποτελεσματικά ή ακατάλληλα για να καλύψουν τους σχετικούς θεμιτούς στόχους της Ένωσης.

(70) Το ευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας θα πρέπει να θεσπιστεί με ενιαίο τρόπο σε όλα τα κράτη μέλη, ώστε να αποφεύγεται η αναζήτηση της πιο συμφέρουσας πιστοποίησης (certification shopping), με βάση τα διάφορα επίπεδα αυστηρότητας σε διαφορετικά κράτη μέλη.

(71) Τα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας θα πρέπει να βασίζονται στα ήδη υπάρχοντα σε διεθνές και εθνικό επίπεδο και, εφόσον απαιτείται, στις τεχνικές προδιαγραφές από φόρουμ και κοινοπραξίες, αντλώντας διδάγματα από τα ισχυρά σημεία και αξιολογώντας και διορθώνοντας τις αδυναμίες.

(72) Οι ευέλικτες λύσεις για την κυβερνοασφάλεια είναι απαραίτητες ώστε ο κλάδος να προλαμβάνει κυβερνοαπειλές και, ως εκ τούτου, κάθε σύστημα πιστοποίησης θα πρέπει είναι σχεδιασμένο έτσι ώστε να αποφεύγεται ο κίνδυνος να καταστεί γρήγορα παρωχημένο.

(73) Η Επιτροπή θα πρέπει να εξουσιοδοτηθεί να εγκρίνει ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας όσον αφορά συγκεκριμένες ομάδες προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ. Τα εν λόγω συστήματα θα πρέπει να εφαρμόζονται και να επιβλέπονται από εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας 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 παρόντος κανονισμού. Ωστόσο, οι οργανισμοί που εφαρμόζουν τέτοια συστήματα θα πρέπει να μπορούν να προτείνουν στην Επιτροπή να εξετάσει αυτά τα συστήματα προκειμένου να εγκριθούν ως ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας.

(74) Οι διατάξεις του παρόντος κανονισμού δεν θα πρέπει να θίγουν το ενωσιακό δίκαιο που προβλέπει συγκεκριμένους κανόνες για την πιστοποίηση προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ. Πιο συγκεκριμένα, ο κανονισμός (ΕΕ) 2016/679 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 ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ. Ο παρών κανονισμός ισχύει με την επιφύλαξη της πιστοποίησης των πράξεων επεξεργασίας των δεδομένων δυνάμει του κανονισμού (ΕΕ) 2016/679, μεταξύ άλλων όταν τέτοιες πράξεις βρίσκονται ενσωματωμένες σε προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ.

(75) Σκοπός των ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας θα πρέπει να είναι να διασφαλίζουν ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ που πιστοποιούνται στο πλαίσιο τέτοιων συστημάτων συμμορφώνονται με συγκεκριμένες απαιτήσεις, σκοπός των οποίων είναι η προστασία της διαθεσιμότητας, της αυθεντικότητας, της ακεραιότητας και της εμπιστευτικότητας αποθηκευμένων, διαβιβαζόμενων ή επεξεργασμένων δεδομένων ή των σχετικών λειτουργιών ή των σχετικών υπηρεσιών που παρέχονται ή είναι προσβάσιμες μέσω των εν λόγω προϊόντων, υπηρεσιών και διαδικασιών καθ' όλη τη διάρκεια του κύκλου ζωής τους. Στον παρόντα κανονισμό δεν είναι δυνατόν να καθοριστούν λεπτομερώς οι απαιτήσεις κυβερνοασφάλειας που σχετίζονται με το σύνολο των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ και των διαδικασιών ΤΠΕ. Τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ και οι σχετικές με τα εν λόγω προϊόντα ανάγκες κυβερνοασφάλειας ποικίλουν σε τέτοιο βαθμό ώστε είναι πολύ δύσκολο να προβλεφθούν γενικές απαιτήσεις κυβερνοασφάλειας που να ισχύουν σε κάθε περίσταση. Επομένως, είναι απαραίτητο να υιοθετηθεί μια ευρεία και γενική έννοια της κυβερνοασφάλειας για τους σκοπούς της πιστοποίησης, η οποία θα πρέπει να συμπληρώνεται από ένα σύνολο συγκεκριμένων στόχων κυβερνοασφάλειας που οφείλεται να συνεκτιμώνται κατά τον σχεδιασμό των ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας. Οι ρυθμίσεις με τις οποίες οφείλεται να επιτυγχάνονται αυτοί οι στόχοι για συγκεκριμένα προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες 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, εάν δεν υπάρχουν διαθέσιμα κατάλληλα πρότυπα.

(76) Οι τεχνικές προδιαγραφές που θα χρησιμοποιηθούν στα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας θα πρέπει να τηρούν τις απαιτήσεις που καθορίζονται στο παράρτημα ΙΙ του κανονισμού (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([19]). Ορισμένες αποκλίσεις από τις εν λόγω απαιτήσεις θα μπορούσαν εντούτοις να θεωρηθούν αναγκαίες σε δεόντως αιτιολογημένες περιπτώσεις όταν οι εν λόγω τεχνικές προδιαγραφές πρόκειται να χρησιμοποιηθούν σε ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας αναφερόμενο σε «υψηλό» επίπεδο διασφάλισης. Οι λόγοι των αποκλίσεων αυτών θα πρέπει να καθίστανται διαθέσιμοι στο κοινό.

(77) Η αξιολόγηση της συμμόρφωσης είναι διαδικασία αξιολόγησης του κατά πόσον πληρούνται οι ειδικές προδιαγραφές που αφορούν ένα προϊόν ΤΠΕ, μια υπηρεσία ΤΠΕ ή μια διαδικασία ΤΠΕ. Η εν λόγω διαδικασία διεξάγεται από ανεξάρτητο τρίτο μέρος, άλλο από τον κατασκευαστή ή τον πάροχο των προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ που αξιολογούνται. Θα πρέπει να εκδίδεται ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας κατόπιν της επιτυχούς αξιολόγησης προϊόντος ΤΠΕ, υπηρεσίας ΤΠΕ ή διαδικασίας ΤΠΕ. Ένα ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας θα πρέπει να θεωρείται ως επιβεβαίωση ότι η αξιολόγηση έχει διενεργηθεί με σωστό τρόπο. Ανάλογα με το επίπεδο διασφάλισης, το ευρωπαϊκό σύστημα πιστοποίησης για την κυβερνοασφάλεια θα πρέπει να επισημαίνει αν το ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας οφείλει να εκδοθεί από ιδιωτικό ή δημόσιο φορέα. Η αξιολόγηση της συμμόρφωσης και η πιστοποίηση δεν μπορούν να εγγυηθούν από μόνες τους ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ που έχουν λάβει πιστοποίηση είναι κυβερνοασφαλή. Πρόκειται μάλλον για διαδικασίες και τεχνικές μεθοδολογίες που βεβαιώνουν ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ έχουν δοκιμαστεί και ότι συμμορφώνονται με ορισμένες απαιτήσεις κυβερνοασφάλειας που προβλέπονται αλλού, για παράδειγμα σε τεχνικά πρότυπα.

(78) Η επιλογή από τους χρήστες των ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας της κατάλληλης πιστοποίησης και των συναφών απαιτήσεων ασφάλειας θα πρέπει να βασίζεται σε ανάλυση των κινδύνων σχετικά με τη χρήση των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ ή των διαδικασιών ΤΠΕ. Κατά συνέπεια, το επίπεδο διασφάλισης θα πρέπει να είναι ανάλογο με το επίπεδο του κινδύνου που συνδέεται με την προβλεπόμενη χρήση του προϊόντος ΤΠΕ, της υπηρεσίας ΤΠΕ ή της διαδικασίας ΤΠΕ.

([19]) Κανονισμός (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Οκτωβρίου 2012, σχετικά με την ευρωπαϊκή τυποποίηση, την τροποποίηση των οδηγιών του Συμβουλίου 89/686/ΕΟΚ και 93/15/ΕΟΚ και των οδηγιών του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου 94/9/ΕΚ, 94/25/ΕΚ, 95/16/ΕΚ, 97/23/ΕΚ, 98/34/ΕΚ, 2004/22/ΕΚ, 2007/23/ΕΚ, 2009/23/ΕΚ και 2009/105/ΕΚ και την κατάργηση της απόφασης 87/95/ΕΟΚ του Συμβουλίου και της απόφασης αριθ. 1673/2006/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (ΕΕ L 316 της 14.11.2012, σ. 12).

(79) Τα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας θα μπορούσαν να προβλέπουν ότι η αξιολόγηση της συμμόρφωσης πραγματοποιείται υπό την αποκλειστική ευθύνη του κατασκευαστή ή του παρόχου προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ («αυτοαξιολόγηση της συμμόρφωσης»). Σε αυτές τις περιπτώσεις, θα πρέπει να αρκεί ο κατασκευαστής ή ο πάροχος προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ να διενεργεί ο ίδιος όλους τους ελέγχους προκειμένου να διασφαλίσει τη συμμόρφωση των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ ή των διαδικασιών ΤΠΕ με το ευρωπαϊκό σύστημα πιστοποίησης όσον αφορά την κυβερνοασφάλεια. Η αυτοαξιολόγηση της συμμόρφωσης θα πρέπει να θεωρείται κατάλληλη για τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ ή τις διαδικασίες ΤΠΕ χαμηλής πολυπλοκότητας που ενέχουν χαμηλό κίνδυνο για το κοινό, όπως οι απλοί μηχανισμοί σχεδιασμού και παραγωγής. Επιπλέον, η αυτοαξιολόγηση της συμμόρφωσης θα πρέπει να επιτρέπεται μόνο για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ ή διαδικασίες ΤΠΕ που αντιστοιχούν στο «βασικό» επίπεδο διασφάλισης.

(80) Τα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας θα μπορούσαν να επιτρέπουν τόσο την αυτοαξιολόγηση της συμμόρφωσης όσον και την πιστοποίηση προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών 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 προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ σχετικά με την αξιολόγηση των οποίων υπεύθυνος είναι ο κατασκευαστής ή ο πάροχος και προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ που λαμβάνουν πιστοποίηση από τρίτο μέρος.

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

(82) Οι κατασκευαστές ή οι πάροχοι προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ θα πρέπει να καθιστούν τη δήλωση συμμόρφωσης ΕΕ, την τεχνική τεκμηρίωση και όλες τις άλλες σχετικές πληροφορίες που αφορούν τη συμμόρφωση των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ ή των διαδικασιών ΤΠΕ με το ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας διαθέσιμα στην αρμόδια εθνική αρχή πιστοποίησης της κυβερνοασφάλειας για διάστημα που προβλέπεται στο σχετικό ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας. Η τεχνική τεκμηρίωση θα πρέπει να προσδιορίζει τις απαιτήσεις που ισχύουν δυνάμει του συστήματος και να καλύπτει τον σχεδιασμό, την κατασκευή και τη λειτουργία του προϊόντος ΤΠΕ, της υπηρεσίας ΤΠΕ ή της διαδικασίας ΤΠΕ στον βαθμό που αυτό απαιτείται για την αυτοαξιολόγηση της συμμόρφωσης. Η τεχνική τεκμηρίωση θα πρέπει να καταρτίζεται με τρόπο ώστε να είναι δυνατή η αξιολόγηση του κατά πόσον ένα προϊόν ΤΠΕ, μια υπηρεσία ΤΠΕ ή μια διαδικασία ΤΠΕ συμμορφώνεται με τις απαιτήσεις που ισχύουν δυνάμει του εν λόγω συστήματος.

(83) Η διακυβέρνηση του ευρωπαϊκού πλαισίου πιστοποίησης της κυβερνοασφάλειας λαμβάνει υπόψη τη συμμετοχή των κρατών μελών, καθώς και την κατάλληλη συμμετοχή των συμφεροντούχων, και καθορίζει τον ρόλο της Επιτροπής κατά τη διάρκεια του σχεδιασμού και της διαμόρφωσης της πρότασης, της αίτησης, της προετοιμασίας, της έγκρισης και της αναθεώρησης ευρωπαϊκού συστήματος πιστοποίησης της κυβερνοασφάλειας.

(84) Η Επιτροπή θα πρέπει να καταρτίσει, με τη στήριξη της ευρωπαϊκής ομάδας πιστοποίησης της κυβερνοασφάλειας («ΕΟΠΙΚ») και της ομάδας συμφεροντούχων για την πιστοποίηση της κυβερνοασφάλειας και μετά από ανοικτή και ευρεία διαβούλευση, ένα κυλιόμενο πρόγραμμα εργασίας της Ένωσης για τα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας και να το δημοσιεύσει υπό μορφή μη δεσμευτικού μέσου. Το κυλιόμενο πρόγραμμα εργασίας της Ένωσης θα πρέπει να είναι στρατηγικό έγγραφο που επιτρέπει ιδίως στον κλάδο, στις εθνικές αρχές και στους οργανισμούς τυποποίησης να προετοιμάζονται εκ των προτέρων για μελλοντικά ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας. Το κυλιόμενο πρόγραμμα εργασίας της Ένωσης θα πρέπει να περιλαμβάνει πολυετή επισκόπηση των αιτημάτων για υποψήφια συστήματα που η Επιτροπή προτίθεται να υποβάλει στον ENISA για επεξεργασία με βάση συγκεκριμένους λόγους. Η Επιτροπή θα πρέπει να λαμβάνει υπόψη το κυλιόμενο πρόγραμμα εργασίας της Ένωσης κατά την εκπόνηση του κυλιόμενου προγράμματός της για την τυποποίηση όσον αφορά τις ΤΠΕ και τα αιτήματα τυποποίησης σε ευρωπαϊκούς οργανισμούς τυποποίησης. Λόγω της ταχείας εισαγωγής και υιοθέτησης νέων τεχνολογιών, λόγω της εμφάνισης άγνωστων μέχρι τώρα κινδύνων για την κυβερνοασφάλεια και λόγω νομοθετικών εξελίξεων και εξελίξεων στην αγορά, η Επιτροπή ή η ΕΟΠΙΚ θα πρέπει να έχει το δικαίωμα να ζητά από τον ENISA να επεξεργάζεται υποψήφια συστήματα τα οποία δεν έχουν περιληφθεί στο κυλιόμενο πρόγραμμα εργασίας της Ένωσης. Στις περιπτώσεις αυτές, η Επιτροπή και η ΕΟΠΙΚ θα πρέπει επίσης να αξιολογεί την αναγκαιότητα του εν λόγω αιτήματος, λαμβάνοντας υπόψη τους γενικούς στόχους και σκοπούς του παρόντος κανονισμού και την ανάγκη διασφάλισης της συνέχειας όσον αφορά τον σχεδιασμό και τη χρήση των πόρων του ENISA.

Κατόπιν τέτοιου αιτήματος, ο ENISA θα πρέπει να επεξεργάζεται, χωρίς αδικαιολόγητη καθυστέρηση, τα υποψήφια συστήματα για συγκεκριμένα προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ. Η Επιτροπή θα πρέπει να αξιολογεί τις θετικές και αρνητικές συνέπειες του αιτήματός της στη συγκεκριμένη αγορά, ιδίως τις συνέπειές του για τις ΜΜΕ, την καινοτομία, τους φραγμούς εισόδου στην εν λόγω αγορά και το κόστος για τους τελικούς χρήστες. Η Επιτροπή, με γνώμονα το υποψήφιο σύστημα που επεξεργάζεται ο ENISA, θα πρέπει να εξουσιοδοτείται να εγκρίνει το ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας μέσω εκτελεστικών πράξεων. Λαμβάνοντας υπόψη τον γενικό σκοπό και τους στόχους ασφάλειας που καθορίζονται στον παρόντα κανονισμό, τα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας 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. Στα εν λόγω στοιχεία θα πρέπει να περιλαμβάνονται, μεταξύ άλλων, το πεδίο εφαρμογής και το αντικείμενο της πιστοποίησης της κυβερνοασφάλειας, συμπεριλαμβανομένων των καλυπτόμενων κατηγοριών προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ, ο λεπτομερής καθορισμός των απαιτήσεων κυβερνοασφάλειας, για παράδειγμα με αναφορά σε πρότυπα ή τεχνικές προδιαγραφές, τα συγκεκριμένα κριτήρια αξιολόγησης και οι μέθοδοι αξιολόγησης, καθώς και το επιθυμητό επίπεδο διασφάλισης («βασικό», «σημαντικό» ή «υψηλό») και τα επίπεδα αξιολόγησης, κατά περίπτωση. Ο ENISA θα πρέπει να δύναται να αρνηθεί αίτημα της ΕΟΠΙΚ. Οι εν λόγω αποφάσεις θα πρέπει να λαμβάνονται από το διοικητικό συμβούλιο και θα πρέπει να είναι δεόντως αιτιολογημένες.

(85) Ο ENISA θα πρέπει να διατηρεί δικτυακό τόπο που να παρέχει πληροφορίες για τα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας και να τα δημοσιεύει, ο οποίος θα πρέπει να περιλαμβάνει, μεταξύ άλλων, τα αιτήματα για την επεξεργασία υποψήφιου συστήματος, καθώς και τις παρατηρήσεις που υποβλήθηκαν κατά τη διαδικασία διαβούλευσης που διενήργησε ο ENISA στη φάση της προετοιμασίας. Ο δικτυακός τόπος θα πρέπει επίσης να παρέχει πληροφορίες σχετικά με τα ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας και τις δηλώσεις συμμόρφωσης ΕΕ που εκδίδονται δυνάμει του παρόντος κανονισμού, μεταξύ άλλων πληροφορίες όσον αφορά την ανάκληση και τη λήξη των εν λόγω ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας και δηλώσεων συμμόρφωσης ΕΕ. Ο δικτυακός τόπος θα πρέπει επίσης να αναφέρει τα εθνικά συστήματα πιστοποίησης κυβερνοασφάλειας που έχουν αντικατασταθεί από ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας.

(86) Το επίπεδο διασφάλισης ευρωπαϊκού συστήματος πιστοποίησης αποτελεί τη βάση για την εμπιστοσύνη ότι ένα προϊόν ΤΠΕ, μια υπηρεσία ΤΠΕ ή μια διαδικασία ΤΠΕ πληροί τις απαιτήσεις ασφαλείας συγκεκριμένου ευρωπαϊκού συστήματος πιστοποίησης της κυβερνοασφάλειας. Προκειμένου να διασφαλισθεί η συνοχή του πλαισίου ευρωπαϊκής πιστοποίησης κυβερνοασφάλειας, ένα ευρωπαϊκό σύστημα πιστοποίησης κυβερνοασφάλειας θα πρέπει να μπορεί να προσδιορίζει τα επίπεδα διασφάλισης των ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας και τις δηλώσεις συμμόρφωσης ΕΕ που εκδίδονται στο πλαίσιο του εν λόγω συστήματος. Κάθε ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας θα μπορεί να αναφέρεται σε ένα από τα επίπεδα διασφάλισης: «βασικό», «ουσιαστικό» ή «υψηλό», ενώ η δήλωση συμμόρφωσης ΕΕ θα μπορεί να αναφέρεται μόνο στο «βασικό» επίπεδο διασφάλισης. Τα επίπεδα διασφάλισης θα παρέχουν την αντίστοιχη αυστηρότητα και βάθος για την αξιολόγηση του προϊόντος ΤΠΕ, της υπηρεσίας ΤΠΕ ή της διαδικασίας ΤΠΕ και θα προσδιορίζονται βάσει σχετικών με αυτά τεχνικών προδιαγραφών, προτύπων και διαδικασιών, συμπεριλαμβανομένων των τεχνικών ελέγχων, σκοπός των οποίων είναι η άμβλυνση ή η πρόληψη συμβάντων. Κάθε επίπεδο διασφάλισης θα πρέπει να είναι συνεπές μεταξύ των διαφόρων τομέων όπου εφαρμόζεται η πιστοποίηση.

(87) Το ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας μπορεί να προσδιορίζει διάφορα επίπεδα αξιολόγησης ανάλογα με την αυστηρότητα και το βάθος της μεθοδολογίας αξιολόγησης που χρησιμοποιείται. Τα επίπεδα αξιολόγησης 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 ΤΠΕ, η υπηρεσία ΤΠΕ ή η διαδικασία ΤΠΕ θα πρέπει να περιέχει μια σειρά ασφαλών λειτουργιών, όπως προσδιορίζονται από το σύστημα, στις οποίες μπορούν να περιλαμβάνονται: εξαρχής ρυθμίσεις ασφαλείας, υπογεγραμμένος κώδικας, ασφαλής επικαιροποίηση/ενημέρωση και περιορισμοί εκμετάλλευσης, καθώς και πλήρεις προστασίες μνήμης σωρού ή 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 λογισμικού και υλισμικού.

(88) Για το «βασικό» επίπεδο διασφάλισης, η αξιολόγηση θα πρέπει να καθοδηγείται τουλάχιστον από τα ακόλουθα συστατικά στοιχεία διασφάλισης: η αξιολόγηση θα πρέπει τουλάχιστον να περιλαμβάνει επανεξέταση των τεχνικών τεκμηριώσεων του προϊόντος ΤΠΕ, της υπηρεσίας ΤΠΕ ή της διαδικασίας ΤΠΕ την οποία διενεργεί ο οργανισμός αξιολόγησης της συμμόρφωσης. Όταν η πιστοποίηση περιλαμβάνει διαδικασίες ΤΠΕ, θα πρέπει να υπόκειται σε τεχνική επανεξέταση η μέθοδος που χρησιμοποιείται για τον σχεδιασμό, την ανάπτυξη και τη διατήρηση προϊόντος ΤΠΕ ή υπηρεσίας ΤΠΕ. Στις περιπτώσεις που ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας προβλέπει αυτοαξιολόγηση της συμμόρφωσης, θα πρέπει να αρκεί το γεγονός ότι ο κατασκευαστής ή ο πάροχος προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ έχει προβεί σε αυτοαξιολόγηση της συμμόρφωσης των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ ή των διαδικασιών ΤΠΕ με το σύστημα πιστοποίησης.

(89) Για το «ουσιαστικό» επίπεδο διασφάλισης, η αξιολόγηση θα πρέπει, επιπλέον των απαιτήσεων για το «βασικό» επίπεδο διασφάλισης, να καθοδηγείται τουλάχιστον από την επαλήθευση της συμμόρφωσης των λειτουργιών ασφαλείας του προϊόντος ΤΠΕ, της υπηρεσίας ΤΠΕ ή της διαδικασίας ΤΠΕ με την οικεία τεχνική τεκμηρίωση.

(90) Για το «υψηλό» επίπεδο διασφάλισης, η αξιολόγηση θα πρέπει, επιπλέον των απαιτήσεων για το «ουσιαστικό» επίπεδο διασφάλισης, να καθοδηγείται τουλάχιστον από δοκιμή απόδοσης, με την οποία αξιολογείται η ανθεκτικότητα των λειτουργιών ασφαλείας του προϊόντος ΤΠΕ, της υπηρεσίας ΤΠΕ ή της διαδικασίας ΤΠΕ έναντι περίτεχνων κυβερνοεπιθέσεων που πραγματοποιούν πρόσωπα τα οποία διαθέτουν σημαντικές δεξιότητες και πόρους.

(91) Η προσφυγή στην ευρωπαϊκή πιστοποίηση της κυβερνοασφάλειας και στις δηλώσεις συμμόρφωσης ΕΕ θα πρέπει να παραμένει εθελοντική, εκτός αν ορίζεται άλλως στο ενωσιακό δίκαιο ή στη νομοθεσία των κρατών μελών που έχει εκδοθεί σύμφωνα με το ενωσιακό δίκαιο. Ελλείψει εναρμονισμένου ενωσιακού δικαίου, τα κράτη μέλη μπορούν να θεσπίζουν εθνικούς τεχνικούς κανονισμούς που προβλέπουν υποχρεωτική πιστοποίηση στο πλαίσιο ευρωπαϊκού συστήματος πιστοποίησης της κυβερνοασφάλειας σύμφωνα με την οδηγία (ΕΕ) 2015/1535 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([20]). Τα κράτη μέλη μπορούν επίσης να προσφεύγουν στην ευρωπαϊκή πιστοποίηση της κυβερνοασφάλειας στο πλαίσιο των δημόσιων συμβάσεων και της οδηγίας 2014/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([21]).

(92) Σε ορισμένους τομείς, μπορεί να χρειαστεί στο μέλλον να επιβληθούν συγκεκριμένες απαιτήσεις κυβερνοασφάλειας και η πιστοποίησή τους να γίνει υποχρεωτική για ορισμένα προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ ή διαδικασίες ΤΠΕ, προκειμένου να βελτιωθεί το επίπεδο κυβερνοασφάλειας στην Ένωση. Η Επιτροπή θα πρέπει να παρακολουθεί τακτικά τις επιπτώσεις των εγκριθέντων ευρωπαϊκών συστημάτων πιστοποίησης κυβερνοασφάλειας στη διαθεσιμότητα ασφαλών προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ στην εσωτερική αγορά και θα πρέπει να αξιολογεί τακτικά το επίπεδο χρησιμοποίησης των συστημάτων πιστοποίησης από τους κατασκευαστές ή τους παρόχους προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ στην Ένωση. Η αποτελεσματικότητα των ευρωπαϊκών συστημάτων πιστοποίησης κυβερνοασφάλειας και το κατά πόσο συγκεκριμένα καθεστώτα θα πρέπει να καταστούν υποχρεωτικά θα πρέπει να αξιολογείται υπό το πρίσμα της νομοθεσίας της Ένωσης που αφορά την κυβερνοασφάλεια, ιδίως της οδηγίας (ΕΕ) 2016/1148, λαμβάνοντας υπόψη την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούνται από τους φορείς εκμετάλλευσης βασικών υπηρεσιών.

(93) Τα ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας και οι δηλώσεις συμμόρφωσης ΕΕ θα πρέπει να βοηθούν τους τελικούς χρήστες να κάνουν εμπεριστατωμένες επιλογές. Συνεπώς, τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ που έχουν υποβληθεί σε πιστοποίηση ή για τα οποία έχει εκδοθεί δήλωση συμμόρφωσης ΕΕ θα πρέπει να συνοδεύονται από δομημένες πληροφορίες, προσαρμοσμένες στο αναμενόμενο τεχνικό επίπεδο του τελικού χρήστη για τον οποίον προορίζονται. Όλες αυτές οι πληροφορίες θα πρέπει να είναι διαθέσιμες επιγραμμικά και, κατά περίπτωση, σε υλική μορφή. Ο τελικός χρήστης θα πρέπει να έχει πρόσβαση σε πληροφορίες όσον αφορά τον αριθμό αναφοράς του συστήματος πιστοποίησης, το επίπεδο διασφάλισης, την περιγραφή των κινδύνων για την κυβερνοασφάλεια που συνδέονται με το προϊόν ΤΠΕ, την υπηρεσία ΤΠΕ ή τη διαδικασία ΤΠΕ και τον οργανισμό ή φορέα έκδοσης ή θα πρέπει να μπορεί να αποκτά αντίγραφο του ευρωπαϊκού πιστοποιητικού κυβερνοασφάλειας. Επιπλέον, ο τελικός χρήστης θα πρέπει να ενημερώνεται για την πολιτική στήριξης της κυβερνοασφάλειας, δηλαδή για πόσο χρονικό διάστημα ο τελικός χρήστης μπορεί να αναμένει ότι θα λαμβάνει ενημερώσεις ή διορθώσεις σχετικές με την κυβερνοασφάλεια, του κατασκευαστή ή του παρόχου προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ. Κατά περίπτωση, θα πρέπει να παρέχεται καθοδήγηση σχετικά με ενέργειες ή ρυθμίσεις που μπορεί να εκτελέσει ο τελικός χρήστης για να διατηρήσει ή να αυξήσει την κυβερνοασφάλεια του προϊόντος ΤΠΕ ή της υπηρεσίας ΤΠΕ και θα πρέπει να παρέχονται πληροφορίες επαφής ενός ενιαίου σημείου επαφής στο οποίο μπορεί να αναφέρει συμβάν και από το οποίο μπορεί να λαμβάνει στήριξη σε περίπτωση κυβερνοεπιθέσεων (πέραν της αυτόματης αναφοράς). Οι εν λόγω πληροφορίες θα πρέπει να επικαιροποιούνται τακτικά και να διατίθενται σε δικτυακό τόπο που να παρέχει πληροφορίες σχετικά με ευρωπαϊκά συστήματα πιστοποίησης κυβερνοασφάλειας.

(94) Προκειμένου να επιτυγχάνονται οι στόχοι του παρόντος κανονισμού και να αποφεύγεται ο κατακερματισμός της εσωτερικής αγοράς, τα εθνικά συστήματα πιστοποίησης της κυβερνοασφάλειας ή οι διαδικασίες για τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ ή τις διαδικασίες ΤΠΕ που καλύπτονται από ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας θα πρέπει να παύουν να ισχύουν από την ημερομηνία που ορίζεται με εκτελεστικές πράξεις από την Επιτροπή. Επιπλέον, τα κράτη μέλη δεν θα πρέπει να θεσπίζουν νέα εθνικά συστήματα πιστοποίησης κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ ή διαδικασίες ΤΠΕ που καλύπτονται ήδη από υφιστάμενο ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας. Ωστόσο, τα κράτη μέλη δεν θα πρέπει να εμποδίζονται να θεσπίζουν ή να διατηρούν εθνικά συστήματα πιστοποίησης κυβερνοασφάλειας για σκοπούς εθνικής ασφάλειας. Τα κράτη μέλη θα πρέπει να ενημερώνουν την Επιτροπή και την ΕΟΠΙΚ για τυχόν πρόθεσή τους να καταρτίσουν νέα εθνικά συστήματα πιστοποίησης της κυβερνοασφάλειας. Η Επιτροπή και η ΕΟΠΙΚ θα πρέπει να αξιολογούν τις επιπτώσεις των νέων εθνικών συστημάτων πιστοποίησης της κυβερνοασφάλειας στην εύρυθμη λειτουργία της εσωτερικής αγοράς και υπό το πρίσμα τυχόν στρατηγικού συμφέροντος να ζητείται, αντί του εθνικού συστήματος, ένα ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας.

(95) Τα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας σκοπό έχουν να συμβάλλουν στην εναρμόνιση των πρακτικών κυβερνοασφάλειας εντός της Ένωσης. Είναι ανάγκη να συμβάλλουν στην αύξηση του επιπέδου κυβερνοασφάλειας εντός της Ένωσης. Ο σχεδιασμός των ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας θα πρέπει να λαμβάνει υπόψη και να επιτρέπει την ανάπτυξη καινοτομιών στον τομέα της κυβερνοασφάλειας.

([20]) Οδηγία (ΕΕ) 2015/1535 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Σεπτεμβρίου 2015, για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προδιαγραφών και των κανόνων σχετικά με τις υπηρεσίες της κοινωνίας των πληροφοριών (ΕΕ L 241 της 17.9.2015, σ. 1).

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

(96) Τα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας θα πρέπει να λαμβάνουν υπόψη τις τρέχουσες μεθόδους ανάπτυξης υλικού και λογισμικού και, ιδίως, τον αντίκτυπο των συχνών ενημερώσεων λογισμικού ή υλικολογισμικού σε ατομικά ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας. Τα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας θα πρέπει να προσδιορίζουν τις συνθήκες υπό τις οποίες, λόγω μιας ενημέρωσης, μπορεί να απαιτηθεί το προϊόν ΤΠΕ, η υπηρεσία ΤΠΕ ή η διαδικασία ΤΠΕ να λάβει εκ νέου πιστοποίηση ή το πεδίο εφαρμογής του συγκεκριμένου ευρωπαϊκού πιστοποιητικού κυβερνοασφάλειας να περιοριστεί, λαμβάνοντας υπόψη ενδεχόμενες δυσμενείς επιπτώσεις της ενημέρωσης στη συμμόρφωση με τις απαιτήσεις ασφάλειας του εν λόγω πιστοποιητικού.

(97) Αφού εγκριθεί ένα ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας, οι πάροχοι ή οι κατασκευαστές προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ θα πρέπει να είναι σε θέση να υποβάλλουν αιτήσεις πιστοποίησης των οικείων προϊόντων ΤΠΕ ή υπηρεσιών ΤΠΕ σε οργανισμό αξιολόγησης της συμμόρφωσης της επιλογής τους οπουδήποτε στην Ένωση. Οι οργανισμοί αξιολόγησης της συμμόρφωσης θα πρέπει να είναι διαπιστευμένοι από εθνικό 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 θα πρέπει να μπορεί να ανανεωθεί με τους ίδιους όρους, υπό την προϋπόθεση ότι ο οργανισμός αξιολόγησης της συμμόρφωσης εξακολουθεί να πληροί τις σχετικές απαιτήσεις. Οι εθνικοί 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 ο οργανισμός αξιολόγησης της συμμόρφωσης παραβαίνει τον παρόντα κανονισμό.

(98) Οι αναφορές της εθνικής νομοθεσίας σε εθνικά πρότυπα τα οποία έχουν παύσει να ισχύουν λόγω της έναρξης ισχύος ενός ευρωπαϊκού συστήματος πιστοποίησης κυβερνοασφάλειας μπορεί να αποτελέσουν πηγή σύγχυσης. Επομένως, η θέσπιση ευρωπαϊκού συστήματος πιστοποίησης της κυβερνοασφάλειας θα πρέπει να αντανακλάται στην εθνική νομοθεσία των κρατών μελών.

(99) Για να επιτευχθούν ισοδύναμα πρότυπα σε ολόκληρη την Ένωση, να διευκολυνθεί η αμοιβαία αναγνώριση και να προαχθεί η γενική αποδοχή των ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας και των δηλώσεων συμμόρφωσης ΕΕ, είναι απαραίτητο να τεθεί σε εφαρμογή ένα σύστημα αξιολόγησης από ομοτίμους μεταξύ εθνικών αρχών πιστοποίησης της κυβερνοασφάλειας. Η αξιολόγηση από ομοτίμους θα πρέπει να καλύπτει τις διαδικασίες για την εποπτεία της συμμόρφωσης των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ και των διαδικασιών ΤΠΕ με τα ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας, για την παρακολούθηση των υποχρεώσεων των κατασκευαστών ή των παρόχων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ οι οποίοι προβαίνουν σε αυτοαξιολόγηση της συμμόρφωσης, για την παρακολούθηση των οργανισμών αξιολόγησης της συμμόρφωσης, καθώς και της καταλληλότητας της εμπειρογνωσίας του προσωπικού των οργανισμών που εκδίδουν πιστοποιητικά για το «υψηλό» επίπεδο διασφάλισης. Η Επιτροπή θα πρέπει να μπορεί να θεσπίσει, με εκτελεστικές πράξεις, τουλάχιστον πενταετές σχέδιο για τις αξιολογήσεις από ομοτίμους, καθώς και να θεσπίσει κριτήρια και μεθοδολογίες για τη λειτουργία του συστήματος αξιολόγησης από ομοτίμους.

(100) Με την επιφύλαξη του γενικού συστήματος αξιολόγησης από ομοτίμους που θα πρέπει να τεθεί σε εφαρμογή σε όλες τις εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας εντός του ευρωπαϊκού πλαισίου πιστοποίησης της κυβερνοασφάλειας, ορισμένα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας μπορούν να περιλαμβάνουν μηχανισμό αξιολόγησης από ομοτίμους για τους οργανισμούς έκδοσης ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ με «υψηλό» επίπεδο διασφάλισης στο πλαίσιο των εν λόγω συστημάτων. Η ΕΟΠΙΚ θα πρέπει να στηρίξει την εφαρμογή τέτοιων μηχανισμών αξιολόγησης από ομοτίμους. Οι αξιολογήσεις από ομοτίμους θα πρέπει ιδίως να αξιολογούν εάν οι σχετικοί οργανισμοί εκτελούν τα καθήκοντά τους εναρμονισμένα και μπορούν να περιλαμβάνουν μηχανισμούς προσφυγής. Τα αποτελέσματα των αξιολογήσεων από ομοτίμους θα πρέπει να δημοσιοποιούνται. Οι ενδιαφερόμενοι οργανισμοί μπορούν να λαμβάνουν κατάλληλα μέτρα για να προσαρμόσουν ανάλογα τις πρακτικές και την εμπειρογνωσία τους.

(101) Τα κράτη μέλη θα πρέπει να ορίζουν μία ή περισσότερες εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας, οι οποίες θα εποπτεύουν τη συμμόρφωση προς τις υποχρεώσεις που απορρέουν από τον παρόντα κανονισμό. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας μπορεί να είναι μια υπάρχουσα ή μια νέα αρχή. Ένα κράτος μέλος θα πρέπει επίσης να είναι σε θέση να ορίζει, κατόπιν συμφωνίας με άλλο κράτος μέλος, μια ή περισσότερες εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας στην επικράτεια του εν λόγω άλλου κράτους μέλους.

(102) Οι εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας θα πρέπει ιδίως να παρακολουθούν και να εφαρμόζουν τις υποχρεώσεις των κατασκευαστών ή των παρόχων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ που είναι εγκατεστημένοι στα αντίστοιχα εδάφη τους σχετικά με τη δήλωση συμμόρφωσης ΕΕ, να επικουρούν τους εθνικούς οργανισμούς διαπίστευσης στην παρακολούθηση και την εποπτεία των δραστηριοτήτων των οργανισμών αξιολόγησης της συμμόρφωσης με την παροχή εμπειρογνωμοσύνης και σχετικών πληροφοριών, να εξουσιοδοτούν τους οργανισμούς αξιολόγησης της συμμόρφωσης για την εκτέλεση των καθηκόντων τους όταν οι εν λόγω οργανισμοί πληρούν τις επιπρόσθετες απαιτήσεις που ορίζονται σε ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας και να παρακολουθούν τις σχετικές εξελίξεις στον τομέα της πιστοποίησης της κυβερνοασφάλειας. Οι εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας θα πρέπει επίσης να χειρίζονται τις καταγγελίες που υποβάλλονται από φυσικά ή νομικά πρόσωπα σε σχέση με ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας που έχουν εκδοθεί από τις εν λόγω αρχές ή σε σχέση με ευρωπαϊκά πιστοποιητικά

κυβερνοασφάλειας που έχουν εκδοθεί από οργανισμούς αξιολόγησης της συμμόρφωσης, όταν τα εν λόγω πιστοποιητικά δείχνουν «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, οι εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας θα πρέπει να συνεργάζονται με άλλες εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας ή άλλες δημόσιες αρχές, μεταξύ άλλων ανταλλάσσοντας πληροφορίες σχετικά με την πιθανή μη συμμόρφωση προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ με τις απαιτήσεις του παρόντος κανονισμού ή συγκεκριμένων ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας. Η Επιτροπή θα πρέπει να διευκολύνει την εν λόγω ανταλλαγή πληροφοριών παρέχοντας ένα γενικό ηλεκτρονικό σύστημα υποστήριξης πληροφοριών, για παράδειγμα το σύστημα πληροφοριών και επικοινωνίας για την εποπτεία της αγοράς (ICSMS) και το σύστημα ταχείας ανταλλαγής πληροφοριών για τους κινδύνους που προκύπτουν από τη χρήση προϊόντων καταναλωτή (RAPEX) που ήδη χρησιμοποιούνται από τις αρχές εποπτείας της αγοράς σύμφωνα με τον κανονισμό (ΕΚ) αριθ. 765/2008.

(103) Για να διασφαλιστεί η συνεκτική εφαρμογή του ευρωπαϊκού πλαισίου πιστοποίησης της κυβερνοασφάλειας, θα πρέπει να δημιουργηθεί ΕΟΠΙΚ η οποία θα απαρτίζεται από εκπροσώπους των εθνικών αρχών πιστοποίησης της κυβερνοασφάλειας ή άλλων αρμόδιων εθνικών αρχών. Κύρια καθήκοντα της ΕΟΠΙΚ θα είναι να συμβουλεύει και να επικουρεί την Επιτροπή στην προσπάθειά της να διασφαλίζει τη συνεπή υλοποίηση και εφαρμογή του ευρωπαϊκού πλαισίου πιστοποίησης της κυβερνοασφάλειας, να παρέχει συνδρομή και να συνεργάζεται στενά με τον ENISA κατά την επεξεργασία των υποψήφιων συστημάτων πιστοποίησης κυβερνοασφάλειας, σε δεόντως αιτιολογημένες περιπτώσεις να ζητεί από τον ENISA την επεξεργασία ενός υποψήφιου συστήματος, να εκδίδει γνώμες απευθυνόμενες στον ENISA για τα υποψήφια συστήματα και να εκδίδει γνώμες απευθυνόμενες στην Επιτροπή όσον αφορά τη διατήρηση και την επανεξέταση υφιστάμενων ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας. Η ΕΟΠΙΚ θα πρέπει να διευκολύνει την ανταλλαγή βέλτιστων πρακτικών και εμπειρογνωμοσύνης μεταξύ των διάφορων εθνικών αρχών πιστοποίησης της κυβερνοασφάλειας οι οποίες είναι αρμόδιες για την εξουσιοδότηση των οργανισμών αξιολόγησης της συμμόρφωσης και την έκδοση των ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας.

(104) Για να προάγει την ευαισθητοποίηση και να διευκολύνει την αποδοχή μελλοντικών ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας, η Επιτροπή μπορεί να εκδίδει γενικές ή ειδικές ανά τομέα κατευθυντήριες γραμμές για την κυβερνοασφάλεια, π.χ. σχετικά με τις ορθές πρακτικές ή την υπεύθυνη συμπεριφορά για την κυβερνοασφάλεια, υπογραμμίζοντας το θετικό αποτέλεσμα από τη χρήση πιστοποιημένων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ.

(105) 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 Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ), συμφωνίες αμοιβαίας αναγνώρισης για τα ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας. Η Επιτροπή, λαμβάνοντας υπόψη τις συμβουλές του ENISA και της ομάδας πιστοποίησης της κυβερνοασφάλειας, δύναται να συστήσει την έναρξη των σχετικών διαπραγματεύσεων. Κάθε ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας θα πρέπει να προβλέπει ειδικούς όρους για τις εν λόγω συμφωνίες αμοιβαίας αναγνώρισης με τρίτες χώρες.

(106) Για τη διασφάλιση ενιαίων προϋποθέσεων εφαρμογής του παρόντος κανονισμού, θα πρέπει να ανατεθούν εκτελεστικές αρμοδιότητες στην Επιτροπή. Οι εν λόγω αρμοδιότητες θα πρέπει να ασκούνται σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 182/2011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([22]).

(107) Η διαδικασία εξέτασης θα πρέπει να χρησιμοποιείται για την έγκριση εκτελεστικών πράξεων σχετικά με τα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ ή διαδικασίες ΤΠΕ, για την έγκριση εκτελεστικών πράξεων σχετικά με τις ρυθμίσεις για τη διενέργεια ερευνών από τον ENISA, για την έγκριση εκτελεστικών πράξεων σχετικά με σχέδιο για την αξιολόγηση από ομοτίμους των εθνικών αρχών πιστοποίησης της κυβερνοασφάλειας, καθώς και για την έγκριση εκτελεστικών πράξεων 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 κυβερνοασφάλειας στην Επιτροπή.

(108) Το έργο του ENISA θα πρέπει να υπόκειται σε τακτική και ανεξάρτητη αξιολόγηση. Στην εν λόγω αξιολόγηση θα πρέπει να λαμβάνονται υπόψη οι στόχοι του ENISA, οι εργασιακές πρακτικές του και η συνάφεια των καθηκόντων του, ιδίως των καθηκόντων του που αφορούν την επιχειρησιακή συνεργασία σε επίπεδο Ένωσης. Η εν λόγω αξιολόγηση θα πρέπει επίσης να εκτιμά τον αντίκτυπο, την αποτελεσματικότητα και την αποδοτικότητα του ευρωπαϊκού πλαισίου πιστοποίησης της κυβερνοασφάλειας. Σε περίπτωση επανεξέτασης, η Επιτροπή θα πρέπει να εξετάζει πώς μπορεί να ενισχυθεί ο ρόλος του ENISA ως σημείου αναφοράς για συμβουλές και εμπειρογνωσία και θα πρέπει επίσης να εξετάζει τη δυνατότητα ανάθεσης στον ENISA υποστηρικτικού ρόλου για την αξιολόγηση προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ τρίτων χωρών που δεν είναι σύμφωνα με τους ενωσιακούς κανόνες, όταν τα εν λόγω προϊόντα, οι υπηρεσίες και οι διαδικασίες εισέρχονται στην Ένωση.

([22]) Κανονισμός (ΕΕ) αριθ. 182/2011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Φεβρουαρίου 2011, για τη θέσπιση κανόνων και γενικών αρχών σχετικά με τους τρόπους ελέγχου από τα κράτη μέλη της άσκησης των εκτελεστικών αρμοδιοτήτων από την Επιτροπή (ΕΕ L 55 της 28.2.2011, σ. 13).

(109) Δεδομένου ότι οι στόχοι του παρόντος κανονισμού δεν μπορούν να επιτευχθούν επαρκώς από τα κράτη μέλη, μπορούν όμως, εξαιτίας της κλίμακας και των επιπτώσεών του, να επιτευχθούν καλύτερα σε επίπεδο της Ένωσης, η Ένωση δύναται να λάβει μέτρα σύμφωνα με την αρχή της επικουρικότητας του άρθρου 5 της Συνθήκης για την Ευρωπαϊκή Ένωση (ΣΕΕ). Σύμφωνα με την αρχή της αναλογικότητας, όπως διατυπώνεται στο ίδιο άρθρο, ο παρών κανονισμός δεν υπερβαίνει τα αναγκαία όρια για την επίτευξη των στόχων αυτών.

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

ΕΞΕΔΩΣΑΝ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

ΤΙΤΛΟΣ I

ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 1

Αντικείμενο και πεδίο εφαρμογής

1. Προκειμένου να διασφαλίζεται η ορθή λειτουργία της εσωτερικής αγοράς, σε συνδυασμό με την επίτευξη ενός υψηλού επιπέδου κυβερνοασφάλειας, κυβερνοανθεκτικότητας και κυβερνοεμπιστοσύνης εντός της Ένωσης, ο παρών κανονισμός θεσπίζει:

α) τους στόχους, τα καθήκοντα και τα οργανωτικά θέματα που σχετίζονται με τον ENISA (ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια) και

β) το πλαίσιο για τη θέσπιση ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας με σκοπό τη διασφάλιση επαρκούς επιπέδου κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ στην Ένωση, καθώς και για τον σκοπό της αποφυγής του κατακερματισμού της εσωτερικής αγοράς όσον αφορά τα συστήματα πιστοποίησης της κυβερνοασφάλειας στην Ένωση.

Το πλαίσιο που αναφέρεται στο στοιχείο β) του πρώτου εδαφίου εφαρμόζεται με την επιφύλαξη των ειδικών διατάξεων σε άλλες νομικές πράξεις της Ένωσης σχετικά με την εθελοντική ή την υποχρεωτική πιστοποίηση.

2. Ο παρών κανονισμός δεν θίγει τις αρμοδιότητες των κρατών μελών σχετικά με 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) «κυβερνοασφάλεια»: οι δραστηριότητες που απαιτούνται για την προστασία των συστημάτων δικτύου και πληροφοριών, των χρηστών των εν λόγω συστημάτων και άλλων επηρεαζόμενων από κυβερνοαπειλές προσώπων,

2) «σύστημα δικτύου και πληροφοριών»: το σύστημα δικτύου και πληροφοριών όπως ορίζεται στο άρθρο 4 σημείο 1) της οδηγίας (ΕΕ) 2016/1148,

3) «εθνική στρατηγική για την ασφάλεια συστημάτων δικτύου και πληροφοριών»: η εθνική στρατηγική για την ασφάλεια συστημάτων δικτύου και πληροφοριών όπως ορίζεται στο άρθρο 4 σημείο 3) της οδηγίας (ΕΕ) 2016/1148,

4) «φορέας εκμετάλλευσης βασικών υπηρεσιών»: ο φορέας εκμετάλλευσης βασικών υπηρεσιών όπως ορίζεται στο άρθρο 4 σημείο 4) της οδηγίας (ΕΕ) 2016/1148,

5) «πάροχος ψηφιακών υπηρεσιών»: ο πάροχος ψηφιακών υπηρεσιών όπως ορίζεται στο άρθρο 4 σημείο 6) της οδηγίας (ΕΕ) 2016/1148,

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

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

8) «κυβερνοαπειλή»: κάθε πιθανή περίσταση, πιθανό συμβάν ή πιθανή ενέργεια που θα μπορούσε να καταστρέψει, να διαταράξει ή να επιδράσει κατ' άλλον τρόπο δυσμενώς στα συστήματα δικτύου και πληροφοριών, στους χρήστες των εν λόγω συστημάτων και σε άλλα πρόσωπα,

9) «ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας»: πλήρες σύνολο κανόνων, τεχνικών απαιτήσεων, προτύπων και διαδικασιών που θεσπίζονται σε επίπεδο Ένωσης και που εφαρμόζονται στην πιστοποίηση ή την αξιολόγηση της συμμόρφωσης συγκεκριμένων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ,

10) «εθνικό σύστημα πιστοποίησης της κυβερνοασφάλειας»: πλήρες σύνολο κανόνων, τεχνικών απαιτήσεων, προτύπων και διαδικασιών που έχουν αναπτυχθεί και εγκριθεί από εθνική δημόσια αρχή και που εφαρμόζονται για την πιστοποίηση ή την αξιολόγηση της συμμόρφωσης των προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ που εμπίπτουν στο πεδίο εφαρμογής του συγκεκριμένου συστήματος,

11) «ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας»: έγγραφο το οποίο εκδίδεται από τον αρμόδιο οργανισμό και βεβαιώνει ότι ένα συγκεκριμένο προϊόν ΤΠΕ, μια συγκεκριμένη υπηρεσία ΤΠΕ ή διαδικασία ΤΠΕ έχει αξιολογηθεί ως προς τη συμμόρφωση με συγκεκριμένες απαιτήσεις ασφαλείας που προβλέπει ένα ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας,

12) «προϊόν ΤΠΕ»: στοιχείο ή ομάδα στοιχείων συστήματος δικτύου ή πληροφοριών,

13) «υπηρεσία ΤΠΕ»: υπηρεσία που συνίσταται εξολοκλήρου ή κατά κύριο λόγο στη διαβίβαση, αποθήκευση, ανάκτηση ή επεξεργασία πληροφοριών μέσω συστημάτων δικτύου και πληροφοριών,

14) «διαδικασία ΤΠΕ»: σύνολο δραστηριοτήτων που διεξάγονται για να σχεδιάζουν, να αναπτύσσουν, να παρέχουν ή να διατηρούν προϊόν ΤΠΕ ή υπηρεσία ΤΠΕ,

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

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

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

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

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

20) «τεχνική προδιαγραφή»: έγγραφο με το οποίο ορίζονται οι τεχνικές απαιτήσεις που πρέπει να πληρούνται από προϊόν ΤΠΕ, υπηρεσία ΤΠΕ ή διαδικασία ΤΠΕ ή οι σχετικές με αυτά διαδικασίες αξιολόγησης της συμμόρφωσης,

21) «επίπεδο διασφάλισης»: η βάση για την εμπιστοσύνη ότι ένα προϊόν ΤΠΕ, μια υπηρεσία ΤΠΕ ή μια διαδικασία ΤΠΕ πληροί τις απαιτήσεις ασφαλείας συγκεκριμένου ευρωπαϊκού συστήματος πιστοποίησης της κυβερνοασφάλειας, το οποίο δείχνει το επίπεδο στο οποίο έχει αξιολογηθεί ένα προϊόν ΤΠΕ, μια υπηρεσία ΤΠΕ ή μια διαδικασία ΤΠΕ αλλά δεν μετρά από μόνο του την ασφάλεια του σχετικού προϊόντος ΤΠΕ, υπηρεσίας ΤΠΕ ή διαδικασίας ΤΠΕ,

22) «αυτοαξιολόγηση της συμμόρφωσης»: ενέργεια που πραγματοποιείται από κατασκευαστή ή πάροχο προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ, η οποία αξιολογεί κατά πόσο τα εν λόγω προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ ή διαδικασίες ΤΠΕ πληρούν τις απαιτήσεις συγκεκριμένου ευρωπαϊκού συστήματος πιστοποίησης της κυβερνοασφάλειας.

ΤΙΤΛΟΣ ΙΙ

ENISA (Ο ΟΡΓΑΝΙΣΜΟΣ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ)

ΚΕΦΑΛΑΙΟ Ι

Εντολή και στόχοι

Άρθρο 3

Εντολή

1. Ο ENISA αναλαμβάνει τα καθήκοντα που του ανατίθενται με τον παρόντα κανονισμό με σκοπό να επιτύχει ένα υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, μεταξύ άλλων υποστηρίζοντας ενεργά τα κράτη μέλη, τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης για τη βελτίωση της κυβερνοασφάλειας. Ο ENISA ενεργεί ως σημείο αναφοράς για την παροχή συμβουλών και εμπειρογνωμοσύνης σχετικά με την κυβερνοασφάλεια για τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης, καθώς και άλλους σχετικούς συμφεροντούχους στην Ένωση.

Ο ENISA συμβάλλει στη μείωση του κατακερματισμού της εσωτερικής αγοράς μέσω της εκτέλεσης των καθηκόντων που του ανατίθενται δυνάμει του παρόντος κανονισμού.

2. Ο ENISA ασκεί καθήκοντα που του ανατίθενται με νομικές πράξεις της Ένωσης που καθορίζουν μέτρα για την προσέγγιση νόμων, κανονισμών και διοικητικών διατάξεων των κρατών μελών που σχετίζονται με την κυβερνοασφάλεια.

3. Κατά την εκτέλεση των καθηκόντων του, ο ENISA ενεργεί ανεξάρτητα, αποφεύγοντας τις αλληλεπικαλύψεις των δραστηριοτήτων των κρατών μελών και λαμβάνοντας υπόψη την υπάρχουσα εμπειρογνωσία των κρατών μελών.

4. Ο ENISA αναπτύσσει τους δικούς του αναγκαίους πόρους, συμπεριλαμβανομένων τεχνικών και ανθρώπινων ικανοτήτων και δεξιοτήτων, για να εκτελεί τα καθήκοντα που του ανατίθενται δυνάμει του παρόντος κανονισμού.

Άρθρο 4

Στόχοι

1. Ο ENISA αποτελεί κέντρο εμπειρογνωσίας σε θέματα κυβερνοασφάλειας χάρη στην ανεξαρτησία του, την επιστημονική και τεχνική ποιότητα των συμβουλών και της επικουρίας που παρέχει, τις πληροφορίες που παρέχει, τη διαφάνεια των επιχειρησιακών διαδικασιών του, τις μεθόδους λειτουργίας και την επιμέλεια με την οποία εκτελεί τα καθήκοντά του.

2. Ο ENISA 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 κυβερνοασφάλεια, συμπεριλαμβανομένων των τομεακών πολιτικών για την κυβερνοασφάλεια.

3. Ο ENISA 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 συμφεροντούχους, με σκοπό την ενίσχυση της προστασίας των συστημάτων δικτύου και πληροφοριών τους, την ανάπτυξη και τη βελτίωση της κυβερνοανθεκτικότητας και της ικανότητας ανταπόκρισης και την ανάπτυξη δεξιοτήτων και ικανοτήτων στο πεδίο της κυβερνοασφάλειας.

4. Ο ENISA προάγει τη συνεργασία, συμπεριλαμβανομένης της ανταλλαγής πληροφοριών, 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 συμφεροντούχους σε θέματα που σχετίζονται με την κυβερνοασφάλεια.

5. Ο ENISA συμβάλλει στην αύξηση των ικανοτήτων κυβερνοασφάλειας σε επίπεδο Ένωσης προκειμένου να στηρίζει τις ενέργειες των κρατών μελών όσον αφορά την πρόληψη και την αντιμετώπιση κυβερνοαπειλών, ιδίως σε περίπτωση διασυνοριακών συμβάντων.

6. Ο ENISA προάγει τη χρήση της ευρωπαϊκής πιστοποίησης της κυβερνοασφάλειας προκειμένου να αποφευχθεί ο κατακερματισμός της εσωτερικής αγοράς. Ο ENISA συμβάλλει στη θέσπιση και τη διατήρηση ενός ευρωπαϊκού πλαισίου πιστοποίησης της κυβερνοασφάλειας σύμφωνα με τον τίτλο ΙΙΙ του παρόντος κανονισμού, προκειμένου να αυξηθεί η διαφάνεια της κυβερνοασφάλειας των προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ και, επομένως, να ενισχυθεί η εμπιστοσύνη στην ψηφιακή εσωτερική αγορά και η ανταγωνιστικότητά της.

7. Ο ENISA προάγει ένα υψηλό επίπεδο ευαισθητοποίησης ως προς την κυβερνοασφάλεια, συμπεριλαμβανομένης της κυβερνοϋγιεινής και του κυβερνογραμματισμού μεταξύ πολιτών, οργανισμών και επιχειρήσεων.

ΚΕΦΑΛΑΙΟ II

Καθήκοντα

Άρθρο 5

Χάραξη και εφαρμογή της πολιτικής και της νομοθεσίας της Ένωσης

Ο ENISA συμβάλλει στη χάραξη και την εφαρμογή της πολιτικής και του δικαίου της Ένωσης:

1) επικουρώντας και παρέχοντας συμβουλές σχετικά με τη χάραξη και την επανεξέταση της πολιτικής και του δικαίου της Ένωσης στον τομέα της κυβερνοασφάλειας και σχετικά με πρωτοβουλίες πολιτικής και δικαίου ανά τομέα εφόσον εμπλέκονται ζητήματα που αφορούν την κυβερνοασφάλεια, ιδίως με την παροχή της οικείας ανεξάρτητης γνωμοδότησης και ανάλυσης, καθώς και με τη διενέργεια προπαρασκευαστικών εργασιών,

2) επικουρώντας τα κράτη μέλη για τη συνεπή εφαρμογή της πολιτικής και του δικαίου της Ένωσης σχετικά με την κυβερνοασφάλεια, ιδίως σε σχέση με την οδηγία (ΕΕ) 2016/1148, μεταξύ άλλων με την έκδοση γνωμοδοτήσεων, κατευθυντήριες γραμμές, την παροχή συμβουλών και βέλτιστων πρακτικών 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) επικουρώντας τα κράτη μέλη και τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης στην ανάπτυξη και την προώθηση πολιτικών κυβερνοασφάλειας που συνδέονται με την υποστήριξη της γενικής διαθεσιμότητας ή της ακεραιότητας του δημόσιου πυρήνα του ανοιχτού διαδικτύου,

4) συμβάλλοντας στο έργο της ομάδας συνεργασίας δυνάμει του άρθρου 11 της οδηγίας (ΕΕ) 2016/1148, παρέχοντας την εμπειρογνωμοσύνη και τη συνδρομή του,

5) στηρίζοντας:

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

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

γ) τα κράτη μέλη στην εφαρμογή των ειδικών πτυχών κυβερνοασφάλειας της πολιτικής και του δικαίου της Ένωσης σχετικά με την προστασία των δεδομένων και της ιδιωτικής ζωής, παρέχοντας συμβουλευτική γνώμη στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων κατόπιν αιτήματος,

6) στηρίζοντας την τακτική επανεξέταση των δραστηριοτήτων πολιτικής της Ένωσης με την εκπόνηση ετήσιας έκθεσης σχετικά με την κατάσταση εφαρμογής του αντίστοιχου νομικού πλαισίου όσον αφορά:

α) πληροφορίες για τις κοινοποιήσεις συμβάντων των κρατών μελών που υποβάλλουν τα ενιαία κέντρα επαφής στην ομάδα συνεργασίας δυνάμει του άρθρου 10 παράγραφος 3 της οδηγίας (ΕΕ) 2016/1148,

β) περιλήψεις των κοινοποιήσεων παραβίασης της ασφάλειας ή απώλειας της ακεραιότητας που λαμβάνονται από παρόχους υπηρεσιών εμπιστοσύνης και που υποβάλλουν τα εποπτικά όργανα στον ENISA, δυνάμει του άρθρου 19 παράγραφος 3 του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([23]),

γ) τις κοινοποιήσεις συμβάντων σχετικών με την ασφάλεια που διαβιβάζουν οι πάροχοι δημόσιων ηλεκτρονικών δικτύων επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, τις οποίες υποβάλλουν οι αρμόδιες αρχές στον Οργανισμό, δυνάμει του άρθρου 40 της οδηγίας (ΕΕ) 2018/1972.

([23]) Κανονισμός (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Ιουλίου 2014, σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ (ΕΕ L 257 της 28.8.2014, σ. 73).

Άρθρο 6

Ανάπτυξη ικανοτήτων

1. Ο ENISA επικουρεί:

α) τα κράτη μέλη στις προσπάθειές τους να βελτιώσουν την ικανότητα πρόληψης, εντοπισμού και ανάλυσης, καθώς και την ικανότητα αντιμετώπισης, κυβερνοαπειλών και συμβάντων, διαθέτοντάς τους τις απαιτούμενες γνώσεις και την απαιτούμενη εμπειρογνωμοσύνη,

β) τα κράτη μέλη και τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης για τη θέσπιση και την εφαρμογή πολιτικών δημοσιοποίησης τρωτών σημείων σε εθελοντική βάση,

γ) τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης στις προσπάθειές τους να βελτιώσουν την ικανότητα πρόληψης, εντοπισμού και ανάλυσης κυβερνοαπειλών και συμβάντων και να βελτιώσουν τις ικανότητές τους αντιμετώπισης τέτοιων κυβερνοαπειλών και συμβάντων, ιδίως με την κατάλληλη υποστήριξη της CERT-EU,

δ) τα κράτη μέλη στην ανάπτυξη εθνικών CSIRT, όταν ζητείται δυνάμει του άρθρου 9 παράγραφος 5 της οδηγίας (ΕΕ) 2016/1148,

ε) τα κράτη μέλη στην ανάπτυξη εθνικών στρατηγικών ασφάλειας των συστημάτων δικτύου και πληροφοριών, όταν ζητείται δυνάμει του άρθρου 7 παράγραφος 2 της οδηγίας (ΕΕ) 2016/1148, και προάγει τη διάδοση των εν λόγω στρατηγικών και σημειώνει την πρόοδο της εφαρμογής τους στην Ένωση, με σκοπό την προαγωγή των βέλτιστων πρακτικών,

στ) τα θεσμικά όργανα της Ένωσης στην ανάπτυξη και την επανεξέταση των ενωσιακών στρατηγικών για την κυβερνοασφάλεια, προάγοντας τη διάδοσή τους και παρακολουθώντας την πρόοδο εφαρμογής τους,

ζ) 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,

η) τα κράτη μέλη μέσω της οργάνωσης τακτικά και τουλάχιστον ανά διετία των ασκήσεων κυβερνοασφάλειας σε επίπεδο Ένωσης που αναφέρονται στο άρθρο 7 παράγραφος 5 και με τη διατύπωση συστάσεων πολιτικής βάσει της διαδικασίας αξιολόγησης των ασκήσεων και των διδαγμάτων που αποκομίζονται από αυτές,

θ) τους αρμόδιους δημόσιους οργανισμούς με την παροχή κατάρτισης σχετικά με την κυβερνοασφάλεια, και αν κρίνεται σκόπιμο σε συνεργασία με τους συμφεροντούχους,

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

2. Ο ENISA 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, τις διαδικασίες, καθώς και για τον τρόπο αντιμετώπισης των ρυθμιστικών ζητημάτων που σχετίζονται με την ανταλλαγή πληροφοριών.

Άρθρο 7

Επιχειρησιακή συνεργασία σε επίπεδο Ένωσης

1. Ο ENISA υποστηρίζει την επιχειρησιακή συνεργασία μεταξύ κρατών μελών, των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης και μεταξύ συμφεροντούχων.

2. Ο ENISA συνεργάζεται σε επιχειρησιακό επίπεδο και αναπτύσσει συνέργειες με τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης, συμπεριλαμβανομένων της CERT-EU, με τις υπηρεσίες που ασχολούνται με το κυβερνοέγκλημα και με τις εποπτικές αρχές που ασχολούνται με την προστασία της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα, με σκοπό την αντιμετώπιση κοινών προβλημάτων, μεταξύ άλλων μέσω:

α) της ανταλλαγής τεχνογνωσίας και βέλτιστων πρακτικών,

β) της παροχής συμβουλών και της έκδοσης κατευθυντήριων γραμμών για συναφή θέματα κυβερνοασφάλειας,

γ) της θέσπισης πρακτικών ρυθμίσεων για την εκτέλεση συγκεκριμένων καθηκόντων κατόπιν διαβούλευσης με την Επιτροπή.

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

4. Ο ENISA στηρίζει τα κράτη μέλη όσον αφορά την επιχειρησιακή συνεργασία εντός του δικτύου CSIRT με:

α) την παροχή συμβουλών για τον τρόπο βελτίωσης των ικανοτήτων τους να προλαμβάνουν, να εντοπίζουν και να αντιμετωπίζουν συμβάντα και, κατόπιν αιτήματος ενός ή περισσοτέρων κρατών μελών, την παροχή συμβουλών σε σχέση με συγκεκριμένη κυβερνοαπειλή,

β) την παροχή συνδρομής, κατόπιν αιτήματος ενός ή περισσοτέρων κρατών μελών, για την εκτίμηση συμβάντων που έχουν σημαντικό ή ουσιαστικό αντίκτυπο, παρέχοντας εμπειρογνωμοσύνη και διευκολύνοντας τον τεχνικό χειρισμό τέτοιων συμβάντων μεταξύ άλλων ιδίως με την παροχή στήριξης για την εθελούσια ανταλλαγή σχετικών πληροφοριών και τεχνικών λύσεων μεταξύ των κρατών μελών,

γ) την ανάλυση τρωτών σημείων και συμβάντων με βάση δημόσια διαθέσιμες πληροφορίες ή πληροφορίες που παρέχονται εθελοντικά από τα κράτη μέλη για τον σκοπό αυτόν και

δ) κατόπιν αιτήματος ενός ή περισσοτέρων κρατών μελών, την παροχή στήριξης σχετικά με τεχνικές εκ των υστέρων έρευνες όσον αφορά συμβάντα με σημαντικό ή ουσιαστικό αντίκτυπο κατά την οδηγία (ΕΕ) 2016/1148.

Κατά την εκτέλεση των εν λόγω καθηκόντων, ο ENISA και η CERT-EU δεσμεύονται σε μια δομημένη συνεργασία προκειμένου να επωφελούνται από τις συνέργειες και να αποφεύγεται η αλληλεπικάλυψη δραστηριοτήτων.

5. Ο ENISA διοργανώνει τακτικά ασκήσεις κυβερνοασφάλειας σε επίπεδο Ένωσης και παρέχει συνδρομή στα κράτη μέλη και τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης στην οργάνωση ασκήσεων κυβερνοασφάλειας κατόπιν αιτήματός τους. Οι εν λόγω ασκήσεις κυβερνοασφάλειας σε επίπεδο Ένωσης είναι δυνατόν να περιλαμβάνουν τεχνικά, επιχειρησιακά και στρατηγικά στοιχεία. Ανά διετία διοργανώνεται από τον ENISA γενική άσκηση μεγάλης κλίμακας.

Κατά περίπτωση, ο ENISA επίσης συμβάλλει και επικουρεί τη διοργάνωση των τομεακών ασκήσεων κυβερνοασφάλειας μαζί με αρμόδιους οργανισμούς που συμμετέχουν επίσης στις ασκήσεις κυβερνοασφάλειας σε επίπεδο Ένωσης.

6. Ο ENISA εκπονεί τακτικά, σε στενή συνεργασία με τα κράτη μέλη, αναλυτική τεχνική έκθεση για την κατάσταση της κυβερνοασφάλειας στην ΕΕ όσον αφορά συμβάντα και κυβερνοαπειλές, με βάση πληροφορίες διαθέσιμες στο κοινό, τις αναλύσεις του και εκθέσεις που υποβάλλουν, μεταξύ άλλων, οι CSIRT των κρατών μελών ή τα ενιαία κέντρα επαφής που ιδρύθηκαν με την οδηγία (ΕΕ) 2016/1148, αμφότερα εθελοντικώς, το EC3 και η CERT-EU.

7. Ο ENISA συμβάλλει στην ανάπτυξη μιας κοινής αντιμετώπισης, σε επίπεδο Ένωσης και κρατών μελών, των μεγάλης κλίμακας διασυνοριακών συμβάντων και κρίσεων που αφορούν την κυβερνοασφάλεια, κυρίως με:

α) τη συγκέντρωση και ανάλυση εκθέσεων από εθνικές πηγές οι οποίες είναι δημόσια διαθέσιμες ή ανταλλάσσονται σε εθελοντική βάση προκειμένου να συνεισφέρει στη δημιουργία κοινής επίγνωσης της κατάστασης,

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

γ) τη διευκόλυνση, κατόπιν αιτήματος, του τεχνικού χειρισμού τέτοιων συμβάντων ή κρίσεων, μεταξύ άλλων ιδίως με την παροχή στήριξης για την εθελούσια ανταλλαγή τεχνικών λύσεων μεταξύ των κρατών μελών,

δ) τη στήριξη των θεσμικών και λοιπών οργάνων και των οργανισμών της Ένωσης και, κατόπιν αιτήματός τους, των κρατών μελών στη δημόσια επικοινωνία σχετικά με τα εν λόγω συμβάντα ή κρίσεις,

ε) τη δοκιμή των σχεδίων συνεργασίας για την αντιμετώπιση τέτοιων συμβάντων ή κρίσεων σε επίπεδο Ένωσης και, κατόπιν αιτήματός τους, την παροχή στήριξης στα κράτη μέλη για να υποβάλουν σε δοκιμές τα σχέδια αυτά σε εθνικό επίπεδο.

Άρθρο 8

Αγορά, πιστοποίηση της κυβερνοασφάλειας και προτυποποίηση

1. Ο ENISA υποστηρίζει και προάγει τη χάραξη και την εφαρμογή της πολιτικής της Ένωσης για την πιστοποίηση της κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ, όπως καθορίζονται στον τίτλο ΙΙΙ του παρόντος κανονισμού:

α) παρακολουθώντας σε συνεχή βάση τις εξελίξεις σε σχετικούς τομείς προτυποποίησης και συνιστώντας κατάλληλες τεχνικές προδιαγραφές για χρήση στην ανάπτυξη ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας δυνάμει του άρθρου 54 παράγραφος 1 στοιχείο γ) σε περιπτώσεις στις οποίες δεν υπάρχουν διαθέσιμα πρότυπα,

β) επεξεργαζόμενος υποψήφια ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας («υποψήφια συστήματα») για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ σύμφωνα με το άρθρο 49,

γ) αξιολογώντας τα εγκριθέντα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας σύμφωνα με το άρθρο 49 παράγραφος 8,

δ) συμμετέχοντας σε αξιολογήσεις από ομοτίμους δυνάμει του άρθρου 59 παράγραφος 4,

ε) επικουρώντας την Επιτροπή, μέσω της παροχής της γραμματειακής υποστήριξης στην ΕΟΠΙΚ δυνάμει του άρθρου 62 παράγραφος 5.

2. Ο ENISA παρέχει τη γραμματειακή υποστήριξη στην ομάδα συμφεροντούχων για την πιστοποίηση της κυβερνοασφάλειας σύμφωνα με το άρθρο 22 παράγραφος 4.

3. Ο ENISA συντάσσει και δημοσιεύει κατευθυντήριες γραμμές και αναπτύσσει ορθές πρακτικές, όσον αφορά τις απαιτήσεις κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ, σε συνεργασία με τις εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας και με τον κλάδο, με τρόπο επίσημο και δομημένο και με διαφάνεια.

4. Ο ENISA συμβάλλει στην επαρκή ανάπτυξη ικανοτήτων σχετικά με διαδικασίες αξιολόγησης και πιστοποίησης με τη συγκέντρωση και την έκδοση κατευθυντηρίων γραμμών, καθώς και με την παροχή στήριξης σε κράτη μέλη κατόπιν αιτήματός τους.

5. Ο ENISA διευκολύνει την καθιέρωση και χρήση ευρωπαϊκών και διεθνών προτύπων για τη διαχείριση κινδύνου και την ασφάλεια των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ και των διαδικασιών ΤΠΕ.

6. Ο ENISA εκπονεί, σε συνεργασία με τα κράτη μέλη και τον κλάδο, 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.

7. Ο ENISA πραγματοποιεί και διαδίδει τακτικές αναλύσεις των κύριων τάσεων στην αγορά της κυβερνοασφάλειας από την πλευρά τόσο της ζήτησης όσο και της προσφοράς, με σκοπό την ενίσχυση της αγοράς κυβερνοασφάλειας εντός της Ένωσης.

Άρθρο 9

Γνώσεις και πληροφορίες

Ο ENISA:

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 κυβερνοασφάλειας,

β) διενεργεί μακροπρόθεσμες στρατηγικές αναλύσεις των κυβερνοαπειλών και των συμβάντων, προκειμένου να εντοπίζει τις αναδυόμενες τάσεις και να συμβάλλει στην πρόληψη συμβάντων,

γ) παρέχει, σε συνεργασία με εμπειρογνώμονες από τις αρχές των κρατών μελών και σχετικούς συμφεροντούχους, 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 χρησιμοποιούνται από τους παρόχους των ψηφιακών υπηρεσιών οι οποίες αναφέρονται στον κατάλογο του παραρτήματος ΙΙΙ της εν λόγω οδηγίας,

δ) μέσω ειδικής διαδικτυακής πύλης, συγκεντρώνει, οργανώνει και γνωστοποιεί στο κοινό πληροφορίες σχετικά με την κυβερνοασφάλεια, τις οποίες παρέχουν τα θεσμικά και λοιπά όργανα και οι οργανισμοί της Ένωσης και πληροφορίες σχετικά με την κυβερνοασφάλεια που παρέχουν, εθελοντικώς, τα κράτη μέλη και ιδιωτικοί και δημόσιοι συμφεροντούχοι,

ε) συλλέγει και αναλύει δημόσια διαθέσιμες πληροφορίες σχετικά με σημαντικά συμβάντα και συντάσσει εκθέσεις με σκοπό την παροχή καθοδήγησης σε πολίτες, οργανισμούς και επιχειρήσεις στην Ένωση.

Άρθρο 10

Ευαισθητοποίηση και εκπαίδευση

Ο ENISA:

α) ευαισθητοποιεί το κοινό σχετικά με τους κινδύνους κυβερνοασφάλειας και παρέχει καθοδήγηση σχετικά με τις ορθές πρακτικές για τους μεμονωμένους χρήστες στοχεύοντας σε πολίτες, οργανισμούς και επιχειρήσεις, συμπεριλαμβανομένης της κυβερνοϋγιεινής και του κυβερνογραμματισμού,

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 κυβερνοασφάλειας και της ορατότητάς της στην Ένωση και ενθαρρύνει την ευρεία δημόσια συζήτηση,

γ) επικουρεί τα κράτη μέλη στις προσπάθειές τους να αυξήσουν την ευαισθητοποίηση για την κυβερνοασφάλεια και να προαγάγουν την εκπαίδευση για την κυβερνοασφάλεια,

δ) στηρίζει τον στενότερο συντονισμό και την ανταλλαγή βέλτιστων πρακτικών μεταξύ των κρατών μελών σχετικά με την ευαισθητοποίηση και την εκπαίδευση για την κυβερνοασφάλεια.

Άρθρο 11

Έρευνα και καινοτομία

Αναφορικά με την έρευνα και καινοτομία, ο ENISA:

α) παρέχει υπηρεσίες συμβούλου στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης και τα κράτη μέλη σχετικά με ερευνητικές ανάγκες και προτεραιότητες στον τομέα της κυβερνοασφάλειας, με σκοπό να καταστεί δυνατή η αποτελεσματική απόκριση στους υπάρχοντες και τους εμφανιζόμενους κινδύνους και τις κυβερνοαπειλές, 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,

γ) συμβάλλει στο στρατηγικό θεματολόγιο για την έρευνα και την καινοτομία σε επίπεδο Ένωσης στον τομέα της κυβερνοασφάλειας.

Άρθρο 12

Διεθνής συνεργασία

Ο ENISA συμβάλλει στις προσπάθειες της Ένωσης για συνεργασία της με τρίτες χώρες και διεθνείς οργανισμούς, μεταξύ άλλων εντός των σχετικών πλαισίων διεθνούς συνεργασίας, για την προώθηση της διεθνούς συνεργασίας σε θέματα που αφορούν την κυβερνοασφάλεια:

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

β) διευκολύνοντας, κατόπιν αιτήματος της Επιτροπής, την ανταλλαγή βέλτιστων πρακτικών,

γ) παρέχοντας, κατόπιν αιτήματός της, εμπειρογνωμοσύνη στην Επιτροπή,

δ) παρέχοντας συμβουλές και στήριξη προς την Επιτροπή σε θέματα σχετικά με συμφωνίες για την αμοιβαία αναγνώριση των πιστοποιητικών κυβερνοασφάλειας με τρίτες χώρες, σε συνεργασία με την ΕΟΠΙΚ που θεσπίζεται σύμφωνα με το άρθρο 62.

ΚΕΦΑΛΑΙΟ III

Οργάνωση του ENISA

Άρθρο 13

Δομή του ENISA

Η δομή διοίκησης και διαχείρισης του ENISA απαρτίζεται από:

α) το διοικητικό συμβούλιο,

β) το εκτελεστικό συμβούλιο,

γ) τον εκτελεστικό διευθυντή,

δ) τη συμβουλευτική ομάδα του ENISA,

ε) δίκτυο εθνικών υπαλλήλων-συνδέσμων.

Τμήμα 1

Διοικητικό Συμβούλιο

Άρθρο 14

Σύνθεση του διοικητικού συμβουλίου

1. Το διοικητικό συμβούλιο απαρτίζεται από ένα μέλος που διορίζεται από κάθε κράτος μέλος και δύο μέλη που διορίζονται από την Επιτροπή. Όλα τα μέλη έχουν δικαίωμα ψήφου.

2. Για κάθε μέλος του διοικητικού συμβουλίου υπάρχει αναπληρωματικό μέλος. Το εν λόγω αναπληρωματικό μέλος εκπροσωπεί το μέλος σε περίπτωση απουσίας του.

3. Τα τακτικά και τα αναπληρωματικά μέλη του διοικητικού συμβουλίου διορίζονται με κριτήριο τη γνώση τους στον τομέα της κυβερνοασφάλειας, 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 αντιπροσώπων τους στο διοικητικό συμβούλιο, προκειμένου να διασφαλίζεται η συνέχεια του έργου του διοικητικού συμβουλίου. 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 15

Καθήκοντα του διοικητικού συμβουλίου

1. Το διοικητικό συμβούλιο:

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

β) εγκρίνει το σχέδιο ενιαίου εγγράφου προγραμματισμού του ENISA που αναφέρεται στο άρθρο 24, πριν από την υποβολή του στην Επιτροπή προκειμένου αυτή να γνωμοδοτήσει σχετικά,

γ) εγκρίνει το ενιαίο έγγραφο προγραμματισμού του ENISA, λαμβάνοντας υπόψη τη γνώμη της Επιτροπής,

δ) επιβλέπει την εφαρμογή του πολυετούς και του ετήσιου προγραμματισμού που περιλαμβάνεται στο ενιαίο έγγραφο προγραμματισμού,

ε) εγκρίνει τον ετήσιο προϋπολογισμό του ENISA και ασκεί άλλες αρμοδιότητες σε σχέση με τον προϋπολογισμό του ENISA σύμφωνα με το κεφάλαιο IV,

στ) αξιολογεί και εγκρίνει την ενοποιημένη ετήσια έκθεση δραστηριοτήτων του ENISA, που περιλαμβάνει τους λογαριασμούς και περιγραφή του τρόπου που ο ENISA έχει επιτύχει τους δείκτες επιδόσεών του, διαβιβάζει την ετήσια έκθεση και την αξιολόγησή του έως την 1η Ιουλίου του επόμενου έτους στο Ευρωπαϊκό Κοινοβούλιο, στο Συμβούλιο, στην Επιτροπή και στο Ελεγκτικό Συνέδριο και δημοσιοποιεί την ετήσια έκθεση,

ζ) θεσπίζει τους δημοσιονομικούς κανόνες που εφαρμόζονται στον ENISA σύμφωνα με το άρθρο 32,

η) χαράσσει στρατηγική καταπολέμησης της απάτης ανάλογη των κινδύνων απάτης και λαμβάνοντας υπόψη την ανάλυση κόστους-οφέλους των ληπτέων μέτρων,

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

ι) 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,

ια) θεσπίζει τον εσωτερικό του κανονισμό, συμπεριλαμβανομένων των κανόνων για προσωρινές αποφάσεις σχετικά με την ανάθεση συγκεκριμένων καθηκόντων, σύμφωνα με το άρθρο 19 παράγραφος 7,

ιβ) όσον αφορά το προσωπικό του ENISA, ασκεί τις εξουσίες που ανατίθενται από τον κανονισμό υπηρεσιακής κατάστασης των υπαλλήλων («κανονισμός υπηρεσιακής κατάστασης των υπαλλήλων») και από το καθεστώς που εφαρμόζεται στο λοιπό προσωπικό της Ευρωπαϊκής Ένωσης («καθεστώς που εφαρμόζεται στο λοιπό προσωπικό»), που καθορίζονται στον κανονισμό (ΕΟΚ, Ευρατόμ, ΕΚΑΧ) αριθ. 259/68 του Συμβουλίου ([24]) στην αρμόδια για τους διορισμούς αρχή και στην αρχή που είναι επιφορτισμένη με τη σύναψη των συμβάσεων προσλήψεως («εξουσίες αρμόδιας για τους διορισμούς αρχής») σύμφωνα με την παράγραφο 2 του παρόντος άρθρου,

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

ιδ) διορίζει τον εκτελεστικό διευθυντή και, ανάλογα με την περίπτωση, παρατείνει τη θητεία του ή τον παύει σύμφωνα με το άρθρο 36,

ιε) 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,

ιστ) λαμβάνει όλες τις αποφάσεις σχετικά με τη συγκρότηση των εσωτερικών δομών του ENISA και, όπου απαιτείται, σχετικά με την τροποποίηση των εν λόγω εσωτερικών δομών, συνεκτιμώντας τις ανάγκες δραστηριοτήτων του ENISA και λαμβάνοντας υπόψη τη χρηστή δημοσιονομική διαχείριση,

ιζ) εγκρίνει τη θέσπιση συμφωνιών συνεργασίας όσον αφορά το άρθρο 7,

ιη) εγκρίνει τη θέσπιση ή τη σύναψη συμφωνιών συνεργασίας σύμφωνα με το άρθρο 42.

2. Σύμφωνα με το άρθρο 110 του κανονισμού υπηρεσιακής κατάστασης, το διοικητικό συμβούλιο εκδίδει απόφαση με βάση το άρθρο 2 παράγραφος 1 του κανονισμού υπηρεσιακής κατάστασης των υπαλλήλων 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.

([24]) ΕΕ L 56 της 4.3.1968, σ. 1.

3. Όταν το επιβάλλουν εξαιρετικές περιστάσεις, το διοικητικό συμβούλιο δύναται να εκδώσει απόφαση προσωρινής αναστολής της μεταβίβασης στον εκτελεστικό διευθυντή των εξουσιών αρμόδιας για τους διορισμούς αρχής και τυχόν εξουσιών αρμόδιας για τους διορισμούς αρχής που ο εκτελεστικός διευθυντής μεταβίβασε περαιτέρω και να τις ασκήσει αντ' αυτού το ίδιο ή να τις αναθέσει σε ένα από τα μέλη του ή σε άλλο μέλος του προσωπικού πλην του εκτελεστικού διευθυντή.

Άρθρο 16

Πρόεδρος του διοικητικού συμβουλίου

Το διοικητικό συμβούλιο εκλέγει με πλειοψηφία των δύο τρίτων των μελών του πρόεδρο και αναπληρωτή πρόεδρο εκ των μελών του. Η θητεία τους είναι 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 αυτεπαγγέλτως τον πρόεδρο, εάν ο πρόεδρος δεν είναι σε θέση να εκτελέσει τα καθήκοντά του.

Άρθρο 17

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 του, κατόπιν αιτήματος της Επιτροπής ή αιτήματος τουλάχιστον ενός τρίτου των μελών του.

3. Ο εκτελεστικός διευθυντής συμμετέχει χωρίς δικαίωμα ψήφου στις συνεδριάσεις του διοικητικού συμβουλίου.

4. Τα μέλη της συμβουλευτικής ομάδας του ENISA 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 δύνανται να επικουρούνται στις συνεδριάσεις του διοικητικού συμβουλίου από συμβούλους ή εμπειρογνώμονες, με την επιφύλαξη του εσωτερικού κανονισμού του διοικητικού συμβουλίου.

6. Ο ENISA παρέχει γραμματειακή υποστήριξη στο διοικητικό συμβούλιο.

Άρθρο 18

Κανόνες ψηφοφορίας του διοικητικού συμβουλίου

1. Το διοικητικό συμβούλιο αποφασίζει με πλειοψηφία των μελών του.

2. Απαιτείται πλειοψηφία δύο τρίτων 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 του διοικητικού συμβουλίου 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.

Τμήμα 2

Εκτελεστικό Συμβούλιο

Άρθρο 19

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) διασφαλίζει, 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 που καθορίζονται στο άρθρο 20, επικουρεί και συμβουλεύει τον εκτελεστικό διευθυντή όσον αφορά την εκτέλεση των αποφάσεων του διοικητικού συμβουλίου για διοικητικά και δημοσιονομικά θέματα σύμφωνα με το άρθρο 20.

3. Το εκτελεστικό συμβούλιο απαρτίζεται από πέντε μέλη. Τα εν λόγω μέλη διορίζονται εκ των μελών του διοικητικού συμβουλίου. Ένα από τα μέλη είναι ο πρόεδρος του διοικητικού συμβουλίου, που μπορεί να ασκεί και την προεδρία του εκτελεστικού συμβουλίου, και ένα άλλο είναι ένας από τους αντιπροσώπους της Επιτροπής. Οι διορισμοί των μελών του εκτελεστικού συμβουλίου επιδιώκουν την ισόρροπη εκπροσώπηση των φύλων στο εκτελεστικό συμβούλιο. Ο εκτελεστικός διευθυντής συμμετέχει στις συνεδριάσεις του εκτελεστικού συμβουλίου χωρίς δικαίωμα ψήφου.

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

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

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

7. Όταν καθίσταται απαραίτητο, λόγω έκτακτης ανάγκης, το εκτελεστικό συμβούλιο δύναται να λάβει ορισμένες προσωρινές αποφάσεις εξ ονόματος του διοικητικού συμβουλίου, ιδίως σε θέματα διοικητικής διαχείρισης, συμπεριλαμβανομένης της αναστολής της μεταβίβασης εξουσιών αρμόδιας για τους διορισμούς αρχής, καθώς και σε θέματα προϋπολογισμού. Οποιεσδήποτε τέτοιες προσωρινές αποφάσεις κοινοποιούνται στο διοικητικό συμβούλιο χωρίς άσκοπη καθυστέρηση. Το διοικητικό συμβούλιο στη συνέχεια αποφασίζει την έγκριση ή την απόρριψη της προσωρινής απόφασης το αργότερο τρεις μήνες μετά τη λήψη της απόφασης. Το εκτελεστικό συμβούλιο δεν λαμβάνει αποφάσεις εκ μέρους του διοικητικού συμβουλίου οι οποίες απαιτούν την έγκριση πλειοψηφίας δύο τρίτων των μελών του διοικητικού συμβουλίου.

Τμήμα 3

Εκτελεστικός διευθυντής

Άρθρο 20

Καθήκοντα του εκτελεστικού διευθυντή

1. Ο ENISA 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 ENISA,

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 ENISA, συμπεριλαμβανομένης της υλοποίησης του ετήσιου προγράμματος εργασίας του ENISA, και την υποβολή της στο διοικητικό συμβούλιο προς αξιολόγηση και έγκριση,

στ) την κατάρτιση σχεδίου δράσης με το οποίο δίνεται συνέχεια στα συμπεράσματα των αναδρομικών αξιολογήσεων και την υποβολή έκθεσης προόδου στην Επιτροπή ανά δύο έτη,

ζ) την κατάρτιση σχεδίου δράσης με το οποίο δίνεται συνέχεια στα πορίσματα εσωτερικών ή εξωτερικών εκθέσεων ελέγχου, καθώς και στις έρευνες της OLAF, και την υποβολή έκθεσης προόδου δύο φορές ετησίως στην Επιτροπή και ανά τακτά χρονικά διαστήματα στο διοικητικό συμβούλιο,

η) την εκπόνηση του σχεδίου των δημοσιονομικών κανόνων που εφαρμόζονται στον ENISA όπως αναφέρονται στο άρθρο 32,

θ) την κατάρτιση του σχεδίου κατάστασης προβλεπόμενων εσόδων και εξόδων του ENISA 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 ENISA, 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 συμφεροντούχους,

ιγ) την τακτική ανταλλαγή απόψεων και πληροφοριών με τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης σχετικά με τις δραστηριότητές τους σχετικά με την κυβερνοασφάλεια προκειμένου να διασφαλίζεται η συνεκτικότητα κατά την ανάπτυξη και εφαρμογή της πολιτικής της Ένωσης,

ιδ) την εκτέλεση άλλων καθηκόντων που ανατίθενται στον εκτελεστικό διευθυντή δυνάμει του παρόντος κανονισμού.

4. Εφόσον κρίνεται αναγκαίο, και στο πλαίσιο της εντολής του ENISA, ο εκτελεστικός διευθυντής μπορεί να συγκροτεί ad hoc ομάδες εργασίας οι οποίες απαρτίζονται από εμπειρογνώμονες, μεταξύ άλλων εμπειρογνώμονες από τις αρμόδιες αρχές των κρατών μελών. Ο εκτελεστικός διευθυντής ενημερώνει σχετικά το διοικητικό συμβούλιο 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 ENISA.

5. Όποτε απαιτείται, για την αποτελεσματική και επαρκή άσκηση των καθηκόντων του ENISA 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 των σχετικών κρατών μελών, συμπεριλαμβανομένου του κράτους μέλους όπου βρίσκεται η έδρα του ENISA, 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 σχετικών κρατών μελών, το θέμα τίθεται προς συζήτηση στο Συμβούλιο. Ο αθροισμένος αριθμός των μελών του προσωπικού σε όλα τα τοπικά γραφεία διατηρείται στο ελάχιστον και δεν υπερβαίνει το 40 % του συνολικού αριθμού των μελών του προσωπικού του ENISA που βρίσκεται στο κράτος μέλος όπου βρίσκεται η έδρα του ENISA. Ο αριθμός των μελών του προσωπικού σε κάθε τοπικό γραφείο δεν υπερβαίνει το 10 % του συνολικού αριθμού των μελών του προσωπικού του ENISA που βρίσκεται στο κράτος μέλος όπου βρίσκεται η έδρα του ENISA.

Στην απόφαση ίδρυσης τοπικού γραφείου 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 ENISA.

Τμήμα 4

Συμβουλευτική Ομάδα του ENISA, ομάδα συμφεροντούχων για την πιστοποίηση της κυβερνοασφάλειας και δίκτυο εθνικών υπαλλήλων-συνδέσμων

Άρθρο 21

Συμβουλευτική ομάδα του ENISA

1. Το διοικητικό συμβούλιο, κατόπιν προτάσεως του εκτελεστικού διευθυντή, συγκροτεί με διαφανή τρόπο τη συμβουλευτική ομάδα του ENISA απαρτιζόμενη από εμπειρογνώμονες εγνωσμένου κύρους που αντιπροσωπεύουν τους σχετικούς συμφεροντούχους, όπως τον κλάδο ΤΠΕ, τους παρόχους δικτύων ή υπηρεσιών ηλεκτρονικών επικοινωνιών για το κοινό, μικρομεσαίες επιχειρήσεις, τους φορείς εκμετάλλευσης βασικών υπηρεσιών, ομάδες καταναλωτών, τους πανεπιστημιακούς που είναι ειδικοί στον τομέα της κυβερνοασφάλειας, και εκπροσώπους των αρμόδιων αρχών στις οποίες υποβάλλεται κοινοποίηση σύμφωνα με την οδηγία (ΕΕ) 2018/1972, ευρωπαϊκών οργανισμών τυποποίησης, όπως επίσης και των αρχών επιβολής του νόμου και των εποπτικών αρχών προστασίας δεδομένων. Το διοικητικό συμβούλιο επιδιώκει να διασφαλίζει κατάλληλη ισορροπία των φύλων και γεωγραφική ισορροπία, καθώς και ισορροπία μεταξύ των διαφόρων ομάδων συμφεροντούχων.

2. Οι διαδικασίες της συμβουλευτικής ομάδας του ENISA, ιδίως όσον αφορά τη σύνθεσή του, την πρόταση του εκτελεστικού διευθυντή που αναφέρεται στην παράγραφο 1, τον αριθμό και τον διορισμό των μελών της, καθώς και τη λειτουργία της συμβουλευτικής ομάδας του ENISA, καθορίζονται στους εσωτερικούς κανόνες λειτουργίας του ENISA και δημοσιοποιούνται.

3. Πρόεδρος της συμβουλευτικής ομάδας του ENISA είναι ο εκτελεστικός διευθυντής ή άλλο πρόσωπο διορισμένο από τον εκτελεστικό διευθυντή κατά περίπτωση.

4. Η διάρκεια της θητείας των μελών της συμβουλευτικής ομάδας του ENISA είναι δυόμισι έτη. Τα μέλη του διοικητικού συμβουλίου δεν είναι μέλη της συμβουλευτικής ομάδας του ENISA. Οι εμπειρογνώμονες της Επιτροπής και των κρατών μελών έχουν δικαίωμα να παρίστανται στις συνεδριάσεις της συμβουλευτικής ομάδας του ENISA και να συμμετέχουν στις εργασίες της. Μπορούν να προσκαλούνται να παρίστανται σε συνεδριάσεις της συμβουλευτικής ομάδας του ENISA και να συμμετέχουν στις εργασίες της εκπρόσωποι άλλων φορέων που δεν είναι μέλη της και κρίνονται σχετικοί από τον εκτελεστικό διευθυντή.

5. Η συμβουλευτική ομάδα του ENISA συμβουλεύει τον ENISA για την εκτέλεση των καθηκόντων του ENISA, με εξαίρεση την εφαρμογή των διατάξεων του τίτλου III του παρόντος κανονισμού. Παρέχει συμβουλές ειδικότερα στον εκτελεστικό διευθυντή κατά την κατάρτιση πρότασης για το ετήσιο πρόγραμμα εργασίας του ENISA και για τη διασφάλιση της επικοινωνίας με τους σχετικούς συμφεροντούχους επί των θεμάτων που σχετίζονται με το ετήσιο πρόγραμμα εργασίας.

6. Η συμβουλευτική ομάδα του ENISA ενημερώνει τακτικά το διοικητικό συμβούλιο για τις δραστηριότητές της.

Άρθρο 22

Ομάδα συμφεροντούχων για την πιστοποίηση της κυβερνοασφάλειας

1. Συστήνεται ομάδα συμφεροντούχων για την πιστοποίηση της κυβερνοασφάλειας.

2. Η ομάδα συμφεροντούχων για την πιστοποίηση της κυβερνοασφάλειας απαρτίζεται από μέλη επιλεγόμενα από εμπειρογνώμονες εγνωσμένου κύρους που εκπροσωπούν τους σχετικούς συμφεροντούχους. Η Επιτροπή, κατόπιν διαφανούς και ανοικτής πρόσκλησης, επιλέγει, κατόπιν προτάσεως του ENISA, τα μέλη της ομάδας συμφεροντούχων για την πιστοποίηση της κυβερνοασφάλειας, διασφαλίζοντας ισορροπία μεταξύ των διάφορων ομάδων συμφεροντούχων, καθώς και κατάλληλη ισορροπία των φύλων και γεωγραφική ισορροπία.

3. Η ομάδα συμφεροντούχων για την πιστοποίηση της κυβερνοασφάλειας:

α) συμβουλεύει την Επιτροπή επί στρατηγικών θεμάτων σχετικά με το ευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας,

β) κατόπιν αιτήματος, ενημερώνει τον ENISA σχετικά με γενικά και στρατηγικά θέματα που αφορούν τα καθήκοντα του ENISA σχετικά με την αγορά, την πιστοποίηση της κυβερνοασφάλειας και την τυποποίηση,

γ) επικουρεί την Επιτροπή στην επεξεργασία του κυλιόμενου προγράμματος εργασίας της Ένωσης που αναφέρεται στο άρθρο 47,

δ) γνωμοδοτεί για το κυλιόμενο πρόγραμμα εργασίας της Ένωσης σύμφωνα με το άρθρο 47 παράγραφος 4 και

ε) σε επείγουσες περιπτώσεις, παρέχει συμβουλές στην Επιτροπή και στην ΕΟΠΙΚ σχετικά με την ανάγκη για επιπρόσθετα συστήματα πιστοποίησης που δεν περιλαμβάνονται στο κυλιόμενο πρόγραμμα εργασίας της Ένωσης, όπως περιγράφεται στα άρθρα 47 και 48.

4. Η ομάδα συμφεροντούχων για την πιστοποίηση της ασφάλειας στον κυβερνοχώρο συμπροεδρεύεται από τους εκπροσώπους της Επιτροπής και του ENISA και ο ENISA εξασφαλίζει τη γραμματεία της.

Άρθρο 23

Δίκτυο εθνικών υπαλλήλων-συνδέσμων

1. Το διοικητικό συμβούλιο, ενεργώντας κατόπιν πρότασης του εκτελεστικού διευθυντή, συγκροτεί δίκτυο εθνικών υπαλλήλων-συνδέσμων, αποτελούμενο από αντιπροσώπους όλων των κρατών μελών (εθνικοί υπάλληλοι-σύνδεσμοι). Κάθε κράτος μέλος ορίζει έναν αντιπρόσωπο στο δίκτυο εθνικών υπαλλήλων-συνδέσμων. Οι συνεδριάσεις του εθνικού δικτύου υπαλλήλων-συνδέσμων μπορούν να διεξάγονται με διάφορες συνθέσεις εμπειρογνωμόνων.

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

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

4. Οι εθνικοί υπάλληλοι-σύνδεσμοι συνεργάζονται στενά με τους αντιπροσώπους των αντίστοιχων κρατών μελών τους στο διοικητικό συμβούλιο, ωστόσο το έργο του ίδιου του δικτύου εθνικών υπαλλήλων-συνδέσμων δεν επικαλύπτει το έργο του διοικητικού συμβουλίου ή άλλων φόρουμ της Ένωσης.

5. Οι αρμοδιότητες και οι διαδικασίες του εθνικού δικτύου υπαλλήλων-συνδέσμων προσδιορίζονται στους εσωτερικούς κανόνες λειτουργίας του ENISA και δημοσιοποιούνται.

Τμήμα 5

Λειτουργία

Άρθρο 24

Ενιαίο έγγραφο προγραμματισμού

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

2. Κάθε χρόνο, ο εκτελεστικός διευθυντής συντάσσει σχέδιο ενιαίου εγγράφου προγραμματισμού που περιέχει το ετήσιο και πολυετές του πρόγραμμα με τον αντίστοιχο προγραμματισμό των οικονομικών και ανθρώπινων πόρων, σύμφωνα με το άρθρο 32 του κατ' εξουσιοδότηση κανονισμού (ΕΕ) αριθ. 1271/2013 της Επιτροπής ([25]) 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 έως τις 31 Ιανουαρίου του επόμενου έτους, καθώς και κάθε μεταγενέστερη επικαιροποιημένη έκδοση του εγγράφου αυτού.

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

([25]) 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).

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.

6. Όταν ανατίθεται στον ENISA 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 67.

Άρθρο 25

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

Άρθρο 26

Διαφάνεια

1. Ο ENISA διεξάγει τις δραστηριότητές του με υψηλό επίπεδο διαφάνειας και σύμφωνα με το άρθρο 28.

2. Ο ENISA 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. Δημοσιοποιεί επίσης τις δηλώσεις συμφερόντων που υποβάλλονται δυνάμει του άρθρου 25.

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

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

Άρθρο 27

Εμπιστευτικότητα

1. Με την επιφύλαξη του άρθρου 28, ο ENISA 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 συμβουλευτικής ομάδας του ENISA, οι εξωτερικοί εμπειρογνώμονες που συμμετέχουν στις ad hoc ομάδες εργασίας, καθώς και τα μέλη του προσωπικού του ENISA, συμπεριλαμβανομένων των υπαλλήλων που αποσπώνται προσωρινά από τα κράτη μέλη, συμμορφώνονται, ακόμη και μετά την παύση των καθηκόντων τους, στις απαιτήσεις τήρησης του απορρήτου του άρθρου 339 ΣΛΕΕ.

3. Ο ENISA 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 ENISA, το διοικητικό συμβούλιο αποφασίζει να επιτρέψει στον ENISA να χειρίζεται διαβαθμισμένες πληροφορίες. Σε αυτή την περίπτωση ο ENISA, κατόπιν συμφωνίας με τις υπηρεσίες της Επιτροπής, εγκρίνει κανόνες ασφάλειας εφαρμόζοντας τις αρχές ασφαλείας που ορίζονται στην απόφαση (ΕΚ, Ευρατόμ) 2015/443 της Επιτροπής ([26]) και στην απόφαση (ΕΚ, Ευρατόμ) 2015/444 της Επιτροπής ([27]). Οι εν λόγω κανόνες ασφάλειας περιλαμβάνουν διατάξεις που έχουν σχέση με την ανταλλαγή, την επεξεργασία και την αποθήκευση διαβαθμισμένων πληροφοριών.

Άρθρο 28

Πρόσβαση σε έγγραφα

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

2. Το διοικητικό συμβούλιο εγκρίνει διατάξεις για την εφαρμογή του κανονισμού (ΕΚ) αριθ. 1049/2001 έως τις 28 Δεκεμβρίου 2019.

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

ΚΕΦΑΛΑΙΟ IV

Κατάρτιση και διάρθρωση του προϋπολογισμού του ENISA

Άρθρο 29

Κατάρτιση του προϋπολογισμού του ENISA

1. Κάθε έτος, ο εκτελεστικός διευθυντής καταρτίζει σχέδιο κατάστασης προβλέψεων των εσόδων και εξόδων του ENISA 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 προβλέψεων, την κατάσταση προβλέψεων των εσόδων και εξόδων του ENISA για το επόμενο οικονομικό έτος.

3. Η κατάσταση προβλέψεων, 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 όπως αναφέρονται στο άρθρο 42 παράγραφος 2.

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

5. Το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο εγκρίνουν τις πιστώσεις για τη συνεισφορά από την Ένωση στον ENISA.

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

([26]) 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).

([27]) 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).

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

Άρθρο 30

Διάρθρωση του προϋπολογισμού του ENISA

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

α) συνεισφορά από τον γενικό προϋπολογισμό της Ένωσης,

β) έσοδα προοριζόμενα για τη χρηματοδότηση συγκεκριμένων δαπανών, σύμφωνα με τους δημοσιονομικούς κανόνες του που αναφέρονται στο άρθρο 32,

γ) χρηματοδότηση από την Ένωση υπό μορφή συμφωνιών ανάθεσης ή ad hoc επιδοτήσεων σύμφωνα με τους δημοσιονομικούς κανόνες που αναφέρονται στο άρθρο 32 και τις διατάξεις των συναφών νομικών πράξεων που πλαισιώνουν τις πολιτικές της Ένωσης,

δ) εισφορές τρίτων χωρών που συμμετέχουν στις εργασίες του ENISA όπως αναφέρεται στο άρθρο 42,

ε) τυχόν εθελοντικές συνεισφορές των κρατών μελών σε χρήματα ή σε είδος.

Τα κράτη μέλη που παρέχουν εθελοντικές συνεισφορές βάσει του στοιχείου ε) του πρώτου εδαφίου δεν αξιώνουν ειδικά δικαιώματα ή υπηρεσίες ως συνέπεια αυτών των συνεισφορών.

2. Στα έξοδα του ENISA 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 31

Εκτέλεση του προϋπολογισμού του ENISA

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

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

3. Ο υπόλογος του ENISA διαβιβάζει τους προσωρινούς λογαριασμούς για το οικονομικό έτος (έτος N) στον υπόλογο της Επιτροπής και στο Ελεγκτικό Συνέδριο έως την 1η Μαρτίου μετά τη λήξη του επόμενου οικονομικού έτους (έτος N + 1).

4. Μετά την παραλαβή των παρατηρήσεων του Ελεγκτικού Συνεδρίου επί των προσωρινών λογαριασμών του ENISA σύμφωνα με το άρθρο 246 του κανονισμού (ΕΕ, Ευρατόμ) 2018/1046 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([28]), ο υπόλογος του ENISA καταρτίζει τους οριστικούς λογαριασμούς του ENISA με δική του ευθύνη και τους υποβάλλει στο διοικητικό συμβούλιο προς γνωμοδότηση.

5. Το διοικητικό συμβούλιο γνωμοδοτεί επί των οριστικών λογαριασμών του ENISA.

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

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

([28]) Κανονισμός (ΕΕ, Ευρατόμ) 2018/1046 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Ιουλίου 2018, σχετικά με τους δημοσιονομικούς κανόνες που εφαρμόζονται στον γενικό προϋπολογισμό της Ένωσης, την τροποποίηση των κανονισμών (ΕΕ) αριθ. 1296/2013, (ΕΕ) αριθ. 1301/2013, (ΕΕ) αριθ. 1303/2013, (ΕΕ) αριθ. 1304/2013, (ΕΕ) αριθ. 1309/2013, (ΕΕ) αριθ. 1316/2013, (ΕΕ) αριθ. 223/2014, (ΕΕ) αριθ. 283/2014 και της απόφασης αριθ. 541/2014/ΕΕ και για την κατάργηση του κανονισμού (ΕΕ, Ευρατόμ) αριθ. 966/2012 (ΕΕ L 193 της 30.7.2018, σ. 1).

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

9. Έως τις 15 Νοεμβρίου του έτους N + 1, ο εκτελεστικός διευθυντής δημοσιεύει τους οριστικούς λογαριασμούς του ENISA στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

10. Έως τις 30 Σεπτεμβρίου του έτους N + 1, ο εκτελεστικός διευθυντής αποστέλλει στο Ελεγκτικό Συνέδριο απάντηση στις παρατηρήσεις του 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 261 παράγραφος 3 του κανονισμού (ΕΕ, Ευρατόμ) 2018/1046.

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

Άρθρο 32

Δημοσιονομικοί κανόνες

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

Άρθρο 33

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 ([29]), ο ENISA έως τις 28 Δεκεμβρίου 2019, προσχωρεί στη διοργανική συμφωνία της 25ης Μαΐου 1999 μεταξύ του Ευρωπαϊκού Κοινοβουλίου, του Συμβουλίου της Ευρωπαϊκής Ένωσης και της Επιτροπής των Ευρωπαϊκών Κοινοτήτων σχετικά με τις εσωτερικές έρευνες που πραγματοποιούνται από την Ευρωπαϊκή Υπηρεσία Καταπολέμησης της Απάτης (OLAF) ([30]). Ο ENISA θεσπίζει τις ενδεδειγμένες διατάξεις που εφαρμόζονται σε όλους τους υπαλλήλους του ENISA, χρησιμοποιώντας το υπόδειγμα που περιλαμβάνεται στο παράρτημα της εν λόγω συμφωνίας.

2. Το Ελεγκτικό Συνέδριο έχει αρμοδιότητα να ελέγχει, βάσει παραστατικών και πληροφοριών που συλλέχθηκαν ως αποτέλεσμα επιτόπιων εξακριβώσεων, όλους τους δικαιούχους, εργολάβους και υπεργολάβους που έλαβαν ενωσιακά κονδύλια από τον ENISA.

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 και στον κανονισμό (Ευρατόμ, ΕΚ) αριθ. 2185/96 του Συμβουλίου ([31]), για τη διαπίστωση τυχόν απάτης, διαφθοράς ή οποιασδήποτε άλλης παράνομης ενέργειας εις βάρος των οικονομικών συμφερόντων της Ένωσης σε σχέση με χρηματοδότηση που παρέχεται στο πλαίσιο επιχορήγησης ή σύμβασης χρηματοδοτούμενης από τον ENISA.

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

([29]) 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 της 18.9.2013, σ. 1).

([30]) ΕΕ L 136 της 31.5.1999, σ. 15.

([31]) 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).

ΚΕΦΑΛΑΙΟ V

Προσωπικό

Άρθρο 34

Γενικές διατάξεις

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

Άρθρο 35

Προνόμια και ασυλίες

Το πρωτόκολλο αριθ. 7 περί των προνομίων και ασυλιών της Ευρωπαϊκής Ένωσης το οποίο προσαρτάται στη ΣΕΕ και στη ΣΛΕΕ εφαρμόζεται στον ENISA και το προσωπικό του.

Άρθρο 36

Εκτελεστικός διευθυντής

1. Ο εκτελεστικός διευθυντής προσλαμβάνεται ως έκτακτος υπάλληλος του ENISA 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 πρόσληψης με τον εκτελεστικό διευθυντή, ο ENISA εκπροσωπείται από τον πρόεδρο του διοικητικού συμβουλίου.

4. Πριν από τον διορισμό, ο υποψήφιος που έχει επιλεγεί από το διοικητικό συμβούλιο καλείται να προβεί σε δήλωση ενώπιον της σχετικής επιτροπής του Ευρωπαϊκού Κοινοβουλίου και να απαντήσει σε ερωτήσεις των βουλευτών.

5. Η θητεία του εκτελεστικού διευθυντή είναι πενταετής. Πριν από τη λήξη αυτής της περιόδου, η Επιτροπή διεξάγει αξιολόγηση των επιδόσεων του εκτελεστικού διευθυντή και των μελλοντικών καθηκόντων και προκλήσεων του ENISA.

6. Οι αποφάσεις του διοικητικού συμβουλίου σχετικά με τον διορισμό, την παράταση της θητείας ή την παύση του εκτελεστικού διευθυντή σύμφωνα με το άρθρο 18 παράγραφος 2.

7. Το διοικητικό συμβούλιο μπορεί, με βάση πρόταση της Επιτροπής στην οποία λαμβάνεται υπόψη η αξιολόγηση που αναφέρεται στην παράγραφο 5, να παρατείνει άπαξ για μια πενταετία τη θητεία του εκτελεστικού διευθυντή.

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 συμμετέχει στη διαδικασία επιλογής για την ίδια θέση.

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

Άρθρο 37

Αποσπασμένοι εμπειρογνώμονες και λοιπό προσωπικό

1. Ο ENISA μπορεί να χρησιμοποιεί αποσπασμένους εθνικούς εμπειρογνώμονες ή άλλο προσωπικό που δεν απασχολείται από τον ENISA. Στο προσωπικό αυτό δεν εφαρμόζονται ο κανονισμός υπηρεσιακής κατάστασης των υπαλλήλων 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 ENISA.

ΚΕΦΑΛΑΙΟ VI

Γενικές διατάξεις που αφορούν τον ENISA

Άρθρο 38

Νομικό καθεστώς του ENISA

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

2. Σε κάθε κράτος μέλος, ο ENISA 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 ENISA εκπροσωπείται από τον εκτελεστικό διευθυντή.

Άρθρο 39

Ευθύνη του ENISA

1. Η συμβατική ευθύνη του ENISA 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 ENISA.

3. Σε περίπτωση μη συμβατικής ευθύνης, ο ENISA 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 σχετική με την αποκατάσταση των ζημιών που αναφέρονται στην παράγραφο 3.

5. Η προσωπική ευθύνη του προσωπικού του ENISA έναντι του ENISA διέπεται από τους σχετικούς όρους που ισχύουν για το προσωπικό του ENISA.

Άρθρο 40

Γλωσσικό καθεστώς

1. Ο ENISA υπόκειται στις διατάξεις του κανονισμού αριθ. 1 του Συμβουλίου ([32]). Τα κράτη μέλη και οι άλλοι φορείς τους οποίους ορίζουν τα κράτη μέλη μπορούν να απευθύνονται στον ENISA και να λαμβάνουν απάντηση στην επίσημη γλώσσα των θεσμικών οργάνων της Ένωσης που επιλέγουν.

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

Άρθρο 41

Προστασία δεδομένων προσωπικού χαρακτήρα

1. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα από τον ENISA υπόκειται στον κανονισμό (ΕΕ) 2018/1725.

2. Το διοικητικό συμβούλιο θεσπίζει τους κανόνες εφαρμογής που αναφέρονται στο άρθρο 45 παράγραφος 3 του κανονισμού (ΕΕ) 2018/1725. Το διοικητικό συμβούλιο μπορεί να θεσπίζει τις πρόσθετες διατάξεις που απαιτούνται για την εφαρμογή του κανονισμού (ΕΕ) 2018/1725 από τον ENISA.

([32]) Κανονισμός αριθ. 1 του Συμβουλίου περί καθορισμού του γλωσσικού καθεστώτος της Ευρωπαϊκής Οικονομικής Κοινότητας (ΕΕ 17 της 6.10.1958, σ. 385/58).

Άρθρο 42

Συνεργασία με τρίτες χώρες και διεθνείς οργανισμούς

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

2. Ο ENISA είναι ανοικτός στη συμμετοχή τρίτων χωρών οι οποίες έχουν συνάψει σχετικές συμφωνίες με την Ένωση. Σύμφωνα με τις σχετικές διατάξεις των εν λόγω συμφωνιών, θεσπίζονται συμφωνίες συνεργασίας που ορίζουν, κυρίως, τη φύση, την έκταση και τον τρόπο συμμετοχής εκάστης των εν λόγω τρίτων χωρών στο έργο του ENISA και περιλαμβάνουν διατάξεις σχετικές με τη συμμετοχή στις πρωτοβουλίες που αναλαμβάνει ο ENISA, την οικονομική συμβολή και το προσωπικό. Στα ζητήματα προσωπικού, οι εν λόγω συμφωνίες συνεργασίας τηρούν πάντοτε τον κανονισμό υπηρεσιακής κατάστασης των υπαλλήλων και το καθεστώς που εφαρμόζεται στο λοιπό προσωπικό.

3. Το διοικητικό συμβούλιο εγκρίνει στρατηγική σχέσεων με τρίτες χώρες και διεθνείς οργανισμούς σχετικά με ζητήματα για τα οποία είναι αρμόδιος ο ENISA. Η Επιτροπή διασφαλίζει ότι ο ENISA λειτουργεί εντός των ορίων της εντολής του και του υπάρχοντος θεσμικού πλαισίου, μέσω της σύναψης κατάλληλης συμφωνίας συνεργασίας με τον εκτελεστικό διευθυντή.

Άρθρο 43

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

Κατόπιν διαβούλευσης με την Επιτροπή, ο ENISA θεσπίζει κανόνες ασφάλειας εφαρμόζοντας τις αρχές ασφάλειας που περιέχονται στους κανόνες ασφάλειας της Επιτροπής σχετικά με την προστασία των ευαίσθητων μη διαβαθμισμένων πληροφοριών και των ΔΠΕΕ που καθορίζονται στις αποφάσεις (ΕΚ, Ευρατόμ) 2015/443 και (ΕΚ, Ευρατόμ) 2015/444. Οι κανόνες ασφάλειας του ENISA περιέχουν διατάξεις για την ανταλλαγή, την επεξεργασία και την αποθήκευση τέτοιων πληροφοριών.

Άρθρο 44

Συμφωνία σχετικά με την έδρα και όροι λειτουργίας

1. Οι απαραίτητες ρυθμίσεις για την εγκατάσταση του ENISA 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 ENISA και τα μέλη των οικογενειών τους, ορίζονται σε συμφωνία για την έδρα η οποία συνάπτεται μεταξύ του ENISA και του κράτους μέλους υποδοχής, μόλις ληφθεί η έγκριση του διοικητικού συμβουλίου.

2. Το κράτος μέλος υποδοχής του ENISA εξασφαλίζει τις καλύτερες δυνατές συνθήκες για τη διασφάλιση της εύρυθμης λειτουργίας του ENISA, λαμβάνοντας υπόψη την προσβασιμότητα του τόπου εγκατάστασης, την ύπαρξη κατάλληλων εκπαιδευτικών δυνατοτήτων για τα τέκνα των υπαλλήλων, την κατάλληλη πρόσβαση στην αγορά εργασίας, την κοινωνική ασφάλιση και την ιατροφαρμακευτική φροντίδα τόσο για τα τέκνα όσο και για τις συζύγους των μελών του προσωπικού.

Άρθρο 45

Διοικητικός έλεγχος

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

ΤΙΤΛΟΣ III

ΠΛΑΙΣΙΟ ΠΙΣΤΟΠΟΙΗΣΗΣ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Άρθρο 46

Ευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας

1. Το ευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας θεσπίζεται με στόχο να βελτιωθούν οι συνθήκες για τη λειτουργία της εσωτερικής αγοράς μέσω αναβάθμισης του επιπέδου κυβερνοασφάλειας εντός της Ένωσης και επιτρέποντας εναρμονισμένη προσέγγιση, σε επίπεδο Ένωσης, των ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας, με απώτερο στόχο τη δημιουργία ψηφιακής ενιαίας αγοράς για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ.

2. Το ευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας προβλέπει ένα μηχανισμό μέσω του οποίου θεσπίζονται ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας και βεβαιώνεται ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ που έχουν αξιολογηθεί σύμφωνα με τα εν λόγω συστήματα συμμορφώνονται με συγκεκριμένες απαιτήσεις ασφάλειας με σκοπό να διαφυλάσσεται η διαθεσιμότητα, η γνησιότητα, η ακεραιότητα και η εμπιστευτικότητα αποθηκευμένων ή διαβιβαζόμενων ή επεξεργασμένων δεδομένων ή των σχετικών λειτουργιών ή υπηρεσιών που παρέχονται ή είναι προσβάσιμες μέσω των εν λόγω προϊόντων, υπηρεσιών και διαδικασιών σε όλη τη διάρκεια του κύκλου ζωής τους.

Άρθρο 47

Το κυλιόμενο πρόγραμμα εργασίας της Ένωσης για την ευρωπαϊκή πιστοποίηση της κυβερνοασφάλειας

1. Η Επιτροπή δημοσιεύει κυλιόμενο πρόγραμμα εργασίας ευρωπαϊκής πιστοποίησης της κυβερνοασφάλειας («κυλιόμενο πρόγραμμα εργασίας της Ένωσης») το οποίο προσδιορίζει στρατηγικές προτεραιότητες για το μέλλον των ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας.

2. Το κυλιόμενο πρόγραμμα εργασίας της Ένωσης περιλαμβάνει ειδικότερα κατάλογο των προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ ή των κατηγοριών τους που μπορούν να έχουν όφελος από τη συμπερίληψή τους στο πεδίο εφαρμογής ευρωπαϊκού συστήματος πιστοποίησης της κυβερνοασφάλειας.

3. Η προσθήκη συγκεκριμένων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ ή κατηγοριών τους στο κυλιόμενο πρόγραμμα εργασίας της Ένωσης αιτιολογείται βάσει ενός ή περισσότερων από τους ακόλουθους λόγους:

α) της διαθεσιμότητας και της ανάπτυξης των εθνικών συστημάτων πιστοποίησης της κυβερνοασφάλειας που καλύπτουν συγκεκριμένη κατηγορία προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ και ιδίως όσον αφορά τον κίνδυνο κατακερματισμού,

β) του σχετικού ενωσιακού δικαίου ή πολιτικής του σχετικού δικαίου ή πολιτικής κράτους μέλους,

γ) της ζήτησης στην αγορά,

δ) των εξελίξεων όσον αφορά τις κυβερνοαπειλές,

ε) αιτήματος για την επεξεργασία συγκεκριμένου υποψήφιου συστήματος από την ΕΟΠΙΚ.

4. Η Επιτροπή λαμβάνει δεόντως υπόψη τις γνωμοδοτήσεις της ΕΟΠΙΚ και της ομάδας συμφεροντούχων για την πιστοποίηση της ασφάλειας στον κυβερνοχώρο σχετικά με το σχέδιο κυλιόμενου προγράμματος εργασίας της Ένωσης.

5. Το πρώτο κυλιόμενο πρόγραμμα εργασίας της Ένωσης δημοσιοποιείται έως τις 28 Ιουνίου 2020. Το κυλιόμενο πρόγραμμα εργασίας της Ένωσης επικαιροποιείται τουλάχιστον μια φορά ανά τριετία και αν κρίνεται απαραίτητο και πιο συχνά.

Άρθρο 48

Αίτημα για ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας

1. Η Επιτροπή μπορεί να ζητήσει από τον ENISA να καταρτίσει υποψήφιο σύστημα ή να επανεξετάσει υφιστάμενο ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας επί τη βάσει του κυλιόμενου προγράμματος εργασίας της Ένωσης.

2. Σε δεόντως αιτιολογημένες περιπτώσεις, η Επιτροπή ή η ΕΟΠΙΚ δύνανται να ζητούν από τον ENISA να καταρτίσει υποψήφιο σύστημα ή να επανεξετάσει υφιστάμενο ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας το οποίο δεν περιλαμβάνεται στο κυλιόμενο πρόγραμμα εργασίας της Ένωσης. Το κυλιόμενο πρόγραμμα εργασίας της Ένωσης επικαιροποιείται αναλόγως.

Άρθρο 49

Επεξεργασία, έγκριση και επανεξέταση ευρωπαϊκού συστήματος πιστοποίησης της κυβερνοασφάλειας

1. Κατόπιν αιτήματος της Επιτροπής σύμφωνα με το άρθρο 48, ο ENISA επεξεργάζεται ένα υποψήφιο σύστημα που πληροί τις απαιτήσεις που ορίζονται στα άρθρα 51, 52 και 54.

2. Κατόπιν αιτήματος της ΕΟΠΙΚ σύμφωνα με το άρθρο 48 παράγραφος 2, ο ENISA μπορεί να επεξεργάζεται ένα υποψήφιο σύστημα που πληροί τις απαιτήσεις που ορίζονται στα άρθρα 51, 52 και 54. Σε περίπτωση που ο ENISA αρνηθεί το εν λόγω αίτημα, εκθέτει τους λόγους της άρνησής του. Κάθε απόφαση άρνησης τέτοιου αιτήματος λαμβάνεται από το διοικητικό συμβούλιο.

3. Κατά την επεξεργασία υποψήφιου συστήματος, ο ENISA διαβουλεύεται με όλους τους σχετικούς συμφεροντούχους μέσω επίσημης, ανοικτής, διαφανούς και χωρίς αποκλεισμούς διαδικασίας διαβούλευσης.

4. Για κάθε υποψήφιο σύστημα, ο ENISA συγκροτεί ad hoc ομάδα εργασίας σύμφωνα με το άρθρο 20 παράγραφος 4 με σκοπό να παρέχει στον ENISA ειδικές συμβουλές και εμπειρογνωμοσύνη.

5. Ο ENISA συνεργάζεται στενά με την ΕΟΠΙΚ. Η ΕΟΠΙΚ παρέχει στον ENISA συνδρομή και εμπειρογνωμοσύνη σε σχέση με την επεξεργασία του υποψήφιου συστήματος και εκδίδει γνώμη σχετικά με το υποψήφιο σύστημα.

6. Ο ENISA λαμβάνει ιδιαιτέρως υπόψη τη γνώμη της ΕΟΠΙΚ προτού διαβιβάσει στην Επιτροπή το υποψήφιο σύστημα που επεξεργάστηκε σύμφωνα τις παραγράφους 3, 4 και 5. Η γνώμη της ΕΟΠΙΚ δεν δεσμεύει τον ENISA, η δε απουσία της εν λόγω γνώμης δεν κωλύει τη διαβίβαση του υποψήφιου συστήματος από τον ENISA στην Επιτροπή.

7. Η Επιτροπή, με βάση το υποψήφιο σύστημα που προετοιμάζει ο ENISA, μπορεί να εκδίδει εκτελεστικές πράξεις οι οποίες προβλέπουν σε σχέση με ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ που πληρούν τις απαιτήσεις των άρθρων 51, 52 και 54. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 66 παράγραφος 2.

8. Ο ENISA επανεξετάζει τουλάχιστον κάθε πέντε έτη όλα τα εγκριθέντα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας, λαμβάνοντας υπόψη τις παρατηρήσεις από τα ενδιαφερόμενα μέρη. Εάν είναι αναγκαίο, η Επιτροπή ή η ΕΟΠΙΚ μπορεί να ζητήσει από τον ENISA να ξεκινήσει τη διαδικασία ανάπτυξης αναθεωρημένου υποψήφιου συστήματος σύμφωνα με τα άρθρο 48 και το παρόν άρθρο.

Άρθρο 50

Δικτυακός τόπος των ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας

1. Ο ENISA διατηρεί ειδικά αφιερωμένο δικτυακό τόπο που έχει πληροφορίες και δημοσιότητα για τα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας, τα ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας και τις δηλώσεις συμμόρφωσης ΕΕ και τα δημοσιοποιεί, συμπεριλαμβανομένων των πληροφοριών όσον αφορά τα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας που δεν ισχύουν πλέον, τα ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας που έχουν ανακληθεί ή λήξει και τις δηλώσεις συμμόρφωσης ΕΕ, καθώς και το αποθετήριο συνδέσμων προς πληροφορίες για την κυβερνοασφάλεια, οι οποίες παρέχονται σύμφωνα με το άρθρο 55.

2. Κατά περίπτωση, ο δικτυακός τόπος που αναφέρεται στην παράγραφο 1 δηλώνει επίσης τα εθνικά συστήματα πιστοποίησης της κυβερνοασφάλειας που έχουν αντικατασταθεί από ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας.

Άρθρο 51

Στόχοι ασφάλειας για τα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας

Ένα ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας 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 του κύκλου ζωής του προϊόντος ΤΠΕ, της υπηρεσίας ΤΠΕ ή της διαδικασίας ΤΠΕ,

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 του κύκλου ζωής του προϊόντος ΤΠΕ, της υπηρεσίας ΤΠΕ ή της διαδικασίας ΤΠΕ,

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

δ) τον εντοπισμό και την τεκμηρίωση γνωστών εξαρτήσεων και τρωτών σημείων,

ε) την καταγραφή των δεδομένων, υπηρεσιών ή λειτουργιών στα οποία πραγματοποιήθηκε πρόσβαση, τα οποία χρησιμοποιήθηκαν ή αποτέλεσαν με άλλον τρόπο αντικείμενο επεξεργασίας, καθώς και του πότε και από ποιον,

στ) 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,

ζ) την επαλήθευση ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ δεν έχουν γνωστά τρωτά σημεία,

η) την έγκαιρη αποκατάσταση της διαθεσιμότητας και της πρόσβασης σε δεδομένα, υπηρεσίες και λειτουργίες σε περίπτωση φυσικού ή τεχνικού συμβάντος,

θ) ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ προστατεύονται εξ ορισμού και από τον σχεδιασμό τους,

ι) ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ παρέχονται με επικαιροποιημένο λογισμικό και υλισμικό που δεν περιέχουν γνωστά στο κοινό τρωτά σημεία, και προβλέπονται μηχανισμοί για ασφαλείς επικαιροποιήσεις.

Άρθρο 52

Επίπεδα διασφάλισης των ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας

1. Ένα ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας μπορεί να προσδιορίζει ένα ή περισσότερα από τα ακόλουθα επίπεδα διασφάλισης για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ: «βασικό», «σημαντικό» ή «υψηλό». Το επίπεδο διασφάλισης είναι ανάλογο του επιπέδου του κινδύνου ο οποίος συνδέεται με την προβλεπόμενη χρήση του προϊόντος ΤΠΕ, της υπηρεσίας ΤΠΕ ή της διαδικασίας ΤΠΕ, από άποψη πιθανότητας και αντικτύπου ενός συμβάντος.

2. Τα ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας και οι δηλώσεις συμμόρφωσης ΕΕ αναφέρουν οποιοδήποτε επίπεδο διασφάλισης που εξειδικεύεται στο ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας υπό το οποίο εκδόθηκε το ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας ή η δήλωση συμμόρφωσης ΕΕ.

3. Οι απαιτήσεις ασφάλειας που αντιστοιχούν σε κάθε επίπεδο διασφάλισης παρέχονται στο σχετικό ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας, συμπεριλαμβανομένων των αντίστοιχων λειτουργιών ασφάλειας και της αντίστοιχης αυστηρότητας και βάθους της αξιολόγησης στην οποία θα υποβληθεί το προϊόν ΤΠΕ, η υπηρεσία ΤΠΕ ή η διαδικασία ΤΠΕ.

4. Το πιστοποιητικό ή η δήλωση συμμόρφωσης ΕΕ αναφέρεται σε τεχνικές προδιαγραφές, πρότυπα και διαδικασίες 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 κυβερνοασφάλεια ή η πρόληψή τους.

5. Ένα ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας ή μία δήλωση συμμόρφωσης ΕΕ που αναφέρεται σε «βασικό» επίπεδο διασφάλισης παρέχει τη διασφάλιση ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ για τα οποία εκδόθηκε το εν λόγω πιστοποιητικό ή η εν λόγω δήλωση συμμόρφωσης ΕΕ πληρούν τις αντίστοιχες απαιτήσεις ασφάλειας, συμπεριλαμβανομένων των λειτουργιών ασφάλειας, και ότι έχουν αξιολογηθεί σε επίπεδο με σκοπό την ελαχιστοποίηση των γνωστών βασικών κινδύνων των συμβάντων και των κυβερνοεπιθέσεων. Οι δραστηριότητες αξιολόγησης που πρόκειται να διεξαχθούν περιλαμβάνουν τουλάχιστον επανεξέταση της τεχνικής τεκμηρίωσης. Εφόσον δεν είναι κατάλληλη τέτοια επανεξέταση, διεξάγονται υποκατάστατες δραστηριότητες αξιολόγησης με ισοδύναμο αποτέλεσμα.

6. Ένα ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας που αναφέρεται σε «σημαντικό» επίπεδο διασφάλισης παρέχει τη διασφάλιση ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ για τα οποία εκδόθηκε το εν λόγω πιστοποιητικό πληρούν τις αντίστοιχες απαιτήσεις ασφάλειας, συμπεριλαμβανομένων των λειτουργιών ασφάλειας, και ότι έχουν αξιολογηθεί σε επίπεδο με σκοπό την ελαχιστοποίηση των γνωστών κινδύνων κυβερνοασφάλειας και του κινδύνου συμβάντων και κυβερνοεπιθέσεων που πραγματοποιούνται από δράστες με περιορισμένες δεξιότητες και πόρους. Οι δραστηριότητες αξιολόγησης που πρόκειται να διεξαχθούν περιλαμβάνουν τουλάχιστον τα ακόλουθα: επανεξέταση για να καταδειχθεί η απουσία γνωστών στο κοινό τρωτών σημείων και έλεγχος για να αποδειχθεί ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ ή οι διαδικασίες ΤΠΕ εφαρμόζουν ορθά την αναγκαία λειτουργία ασφάλειας. Εφόσον οποιεσδήποτε τέτοιες δραστηριότητες αξιολόγησης δεν είναι κατάλληλες, διεξάγονται υποκατάστατες δραστηριότητες αξιολόγησης με ισοδύναμο αποτέλεσμα.

7. Ένα ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας που αναφέρεται σε «υψηλό» επίπεδο διασφάλισης παρέχει τη διασφάλιση ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ για τα οποία εκδόθηκε το εν λόγω πιστοποιητικό πληρούν τις αντίστοιχες απαιτήσεις ασφάλειας, συμπεριλαμβανομένων των λειτουργιών ασφάλειας, και ότι έχουν αξιολογηθεί σε επίπεδο με σκοπό την ελαχιστοποίηση του κινδύνου κυβερνοεπιθέσεων προηγμένης τεχνολογίας που πραγματοποιούνται από δράστες με σημαντικές δεξιότητες και πόρους. Οι δραστηριότητες αξιολόγησης που πρόκειται να διεξαχθούν περιλαμβάνουν τουλάχιστον τα ακόλουθα: επανεξέταση για να καταδειχθεί η απουσία γνωστών στο κοινό τρωτών σημείων, έλεγχος για να αποδειχθεί ότι τα προϊόντα ΤΠΕ, οι διαδικασίες ΤΠΕ και οι υπηρεσίες ΤΠΕ εφαρμόζουν ορθά την αναγκαία λειτουργία ασφάλειας προηγμένης τεχνολογίας και εκτίμηση της ανθεκτικότητάς τους σε επιδέξιους επιτιθέμενους μέσω δοκιμών διείσδυσης. Εφόσον οποιεσδήποτε τέτοιες δραστηριότητες αξιολόγησης δεν είναι κατάλληλες, διεξάγονται υποκατάστατες δραστηριότητες αξιολόγησης με ισοδύναμο αποτέλεσμα.

8. Ένα ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας μπορεί να προσδιορίζει διάφορα επίπεδα αξιολόγησης ανάλογα με την αυστηρότητα και το βάθος της μεθοδολογίας αξιολόγησης που χρησιμοποιείται. Καθένα από τα επίπεδα αξιολόγησης αντιστοιχεί σε ένα από τα επίπεδα διασφάλισης και ορίζεται από κατάλληλο συνδυασμό συστατικών διασφάλισης.

Άρθρο 53

Αυτοαξιολόγηση της συμμόρφωσης

1. Ένα ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας μπορεί να επιτρέπει την αυτοαξιολόγησης της συμμόρφωσης υπό την αποκλειστική ευθύνη του κατασκευαστή ή του παρόχου προϊόντων ΤΠΕΡ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ. Η αυτοαξιολόγηση της συμμόρφωσης επιτρέπεται μόνο σχετικά με προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ χαμηλού κινδύνου που αντιστοιχούν σε «βασικό» επίπεδο διασφάλισης.

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

3. Ο κατασκευαστής ή ο πάροχος προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ καθιστά τη δήλωση συμμόρφωσης ΕΕ, την τεχνική τεκμηρίωση και όλες τις άλλες σχετικές πληροφορίες που αφορούν τη συμμόρφωση των προϊόντων ΤΠΕ ή των υπηρεσιών ΤΠΕ με το σύστημα διαθέσιμα στην εθνική αρχή πιστοποίησης της κυβερνοασφάλειας που αναφέρεται στο άρθρο 58 για περίοδο που καθορίζεται στο αντίστοιχο ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας. Αντίγραφο της δήλωσης συμμόρφωσης ΕΕ υποβάλλεται στην εθνική αρχή πιστοποίησης της κυβερνοασφάλειας και στον ENISA.

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

5. Η δήλωση συμμόρφωσης ΕΕ αναγνωρίζεται σε όλα τα κράτη μέλη.

Άρθρο 54

Στοιχεία των ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας

1. Ένα ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας περιλαμβάνει τουλάχιστον τα ακόλουθα στοιχεία:

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

β) επακριβή περιγραφή του σκοπού του συστήματος και του τρόπου με τον οποίο τα επιλεγέντα πρότυπα, οι μέθοδοι αξιολόγησης και τα επίπεδα διασφάλισης αντιστοιχούν στις ανάγκες των προβλεπόμενων χρηστών του συστήματος,

γ) αναφορά σε διεθνή, ευρωπαϊκά ή εθνικά πρότυπα που εφαρμόζονται κατά την αξιολόγηση ή, όταν δεν υπάρχουν ή δεν ενδείκνυνται τέτοια πρότυπα, σε τεχνικές προδιαγραφές που πληρούν τις απαιτήσεις που καθορίζονται στο παράρτημα ΙΙ του κανονισμού (ΕΕ) αριθ. 1025/2012 ή, εάν δεν υπάρχουν τέτοιες προδιαγραφές, σε τεχνικές προδιαγραφές ή άλλες απαιτήσεις κυβερνοασφάλειας που ορίζονται στο ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας,

δ) όπου συντρέχει περίπτωση, ένα ή περισσότερα επίπεδα διασφάλισης,

ε) ένδειξη του αν η αυτοαξιολόγηση της συμμόρφωσης επιτρέπεται στο πλαίσιο του συστήματος,

στ) κατά περίπτωση, τις ειδικές ή πρόσθετες απαιτήσεις στις οποίες υπόκεινται οι οργανισμοί αξιολόγησης της συμμόρφωσης προκειμένου να διασφαλίζεται η τεχνική ικανότητά τους να αξιολογούν τις απαιτήσεις κυβερνοασφάλειας,

ζ) τα ειδικά κριτήρια και τις μεθόδους αξιολόγησης που πρόκειται να χρησιμοποιούνται, συμπεριλαμβανομένων των τύπων αξιολόγησης, προκειμένου να καταδεικνύεται ότι επιτυγχάνονται οι στόχοι ασφάλειας που αναφέρονται στο άρθρο 51,

η) κατά περίπτωση, τις πληροφορίες που είναι απαραίτητες για την πιστοποίηση και που πρέπει να παρέχονται ή άλλως τίθενται στη διάθεση των οργανισμών αξιολόγησης της συμμόρφωσης από κάποιον αιτούντα,

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

ι) τους κανόνες παρακολούθησης της συμμόρφωσης των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ και των διαδικασιών ΤΠΕ με τις απαιτήσεις των ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας ή των δηλώσεων συμμόρφωσης ΕΕ, συμπεριλαμβανομένων των μηχανισμών για την κατάδειξη της συνεχούς συμμόρφωσης με τις συγκεκριμένες απαιτήσεις της κυβερνοασφάλειας,

ια) κατά περίπτωση, τις προϋποθέσεις για την έκδοση, τη διατήρηση, τη συνέχιση και την ανανέωση ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας, καθώς και τις προϋποθέσεις για την επέκταση ή τον περιορισμό του πεδίου εφαρμογής της πιστοποίησης,

ιβ) τους κανόνες σχετικά με τις συνέπειες προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ που έχουν πιστοποιηθεί ή για τα οποία έχει εκδοθεί δήλωση συμμόρφωσης ΕΕ τα οποία όμως δεν συμμορφώνονται προς τις απαιτήσεις του συστήματος,

ιγ) τους κανόνες σχετικά με τον τρόπο που τα προηγουμένως μη διαπιστωθέντα σχετικά με την κυβερνοασφάλεια τρωτά σημεία προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ πρέπει να αναφέρονται και να αντιμετωπίζονται,

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

ιε) τον προσδιορισμό εθνικών ή διεθνών συστημάτων πιστοποίησης της κυβερνοασφάλειας που καλύπτουν τον ίδιο τύπο ή τις ίδιες κατηγορίες προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ, απαιτήσεις ασφάλειας, κριτήρια και μεθόδους αξιολόγησης και επίπεδα διασφάλισης,

ιστ) το περιεχόμενο και τον μορφότυπο των ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας και των δηλώσεων συμμόρφωσης ΕΕ που πρόκειται να εκδοθούν,

ιζ) την περίοδο διαθεσιμότητας της δήλωσης συμμόρφωσης ΕΕ, την τεχνική τεκμηρίωση και όλες τις άλλες σχετικές πληροφορίες που πρέπει να καταστούν διαθέσιμες από τον κατασκευαστή ή τον πάροχο προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ,

ιη) τη μέγιστη περίοδο ισχύος ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας που εκδίδονται δυνάμει του συστήματος,

ιθ) την πολιτική κοινοποίησης για ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας που έχουν εκδοθεί, τροποποιηθεί ή ανακληθεί δυνάμει του συστήματος,

κ) τις προϋποθέσεις για την αμοιβαία αναγνώριση συστημάτων πιστοποίησης με τρίτες χώρες,

κα) κατά περίπτωση, τους κανόνες σχετικά με τυχόν μηχανισμό αξιολόγησης από ομοτίμους που θεσπίζεται στο πλαίσιο του συστήματος όσον αφορά τις αρχές ή τους οργανισμούς που εκδίδουν ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας για «υψηλό» επίπεδο διασφάλισης δυνάμει του άρθρου 56 παράγραφος 6. Ο μηχανισμός αυτός εφαρμόζεται με την επιφύλαξη της αξιολόγησης από ομοτίμους που προβλέπεται στο άρθρο 59,

κβ) τον μορφότυπο και τις διαδικασίες που πρέπει να τηρούν οι κατασκευαστές ή οι πάροχοι προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ στην παροχή και επικαιροποίηση των συμπληρωματικών πληροφοριών για την κυβερνοασφάλεια σύμφωνα με το άρθρο 55.

2. Οι καθορισμένες απαιτήσεις του ευρωπαϊκού συστήματος πιστοποίησης της κυβερνοασφάλειας συνάδουν με τυχόν εφαρμοστέες νομικές απαιτήσεις, ιδίως όσον αφορά απαιτήσεις προερχόμενες από το εναρμονισμένο ενωσιακό δίκαιο.

3. Σε περίπτωση που κάτι τέτοιο προβλέπεται από συγκεκριμένη νομική πράξη της Ένωσης, πιστοποιητικό ή δήλωση συμμόρφωσης ΕΕ που εκδίδεται στο πλαίσιο ενός ευρωπαϊκού συστήματος πιστοποίησης της κυβερνοασφάλειας μπορεί να χρησιμοποιείται για να καταδεικνύει το τεκμήριο συμμόρφωσης με τις απαιτήσεις της εν λόγω νομικής πράξης.

4. Εφόσον δεν υπάρχει εναρμονισμένο ενωσιακό δίκαιο, το δίκαιο των κρατών μελών μπορεί επίσης να προβλέπει ότι ένα ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας μπορεί να χρησιμοποιείται για τη θέσπιση του τεκμήριου συμμόρφωσης με τις νομικές απαιτήσεις.

Άρθρο 55

Συμπληρωματικές πληροφορίες σχετικά με την κυβερνοασφάλεια για πιστοποιημένα προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ

1. Ο κατασκευαστής ή ο πάροχος πιστοποιημένων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ ή προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ για τα οποία έχει εκδοθεί δήλωση συμμόρφωσης ΕΕ δημοσιοποιεί τις ακόλουθες συμπληρωματικές πληροφορίες σχετικά με την κυβερνοασφάλεια:

α) καθοδήγηση και συστάσεις για τη συνδρομή προς τους τελικούς χρήστες ως προς τις ασφαλείς ρυθμίσεις, την εγκατάσταση, τη διάθεση, τη λειτουργία και τη συντήρηση των προϊόντων ΤΠΕ ή των υπηρεσιών ΤΠΕ,

β) την περίοδο κατά την οποία θα προσφέρεται υποστήριξη ασφαλείας προς τους τελικούς χρήστες, ιδίως όσον αφορά τη διαθεσιμότητα επικαιροποιήσεων σχετικών με την κυβερνοασφάλεια,

γ) τα στοιχεία επικοινωνίας του κατασκευαστή ή του παρόχου και τις αποδεκτές μεθόδους για τη λήψη πληροφοριών από τελικούς χρήστες και ερευνητές ασφαλείας σχετικά με τρωτά σημεία,

δ) παραπομπή σε επιγραμμικά αποθετήρια με καταλόγους δημοσιοποιημένων τρωτών σημείων που συνδέονται με το προϊόν ΤΠΕ, την υπηρεσία ΤΠΕ ή τη διαδικασία ΤΠΕ και σε οποιεσδήποτε συμβουλές σχετικά με την κυβερνοασφάλεια.

2. Οι πληροφορίες που αναφέρονται στην παράγραφο 1 διατίθενται σε ηλεκτρονική μορφή και παραμένουν διαθέσιμες και ενημερωμένες, στον βαθμό που απαιτείται, τουλάχιστον μέχρι τη λήξη του αντίστοιχου ευρωπαϊκού πιστοποιητικού κυβερνοασφάλειας ή της αντίστοιχης δήλωσης συμμόρφωσης ΕΕ.

Άρθρο 56

Πιστοποίηση της κυβερνοασφάλειας

1. Τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ που έχουν πιστοποιηθεί στο πλαίσιο ενός ευρωπαϊκού συστήματος πιστοποίησης της κυβερνοασφάλειας που εγκρίνεται δυνάμει του άρθρου 49 τεκμαίρονται ότι πληρούν τις απαιτήσεις ενός τέτοιου συστήματος.

2. Η πιστοποίηση της κυβερνοασφάλειας είναι εθελοντική, εκτός αν άλλως ορίζεται στο δίκαιο της Ένωσης ή στο δίκαιο των κρατών μελών.

3. Η Επιτροπή αξιολογεί τακτικά την απόδοση και τη χρήση των εγκριθέντων ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας, καθώς και αν συγκεκριμένα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας πρόκειται να καταστούν υποχρεωτικά μέσω συναφούς ενωσιακού δικαίου προκειμένου να διασφαλίζεται επαρκές επίπεδο κυβερνοασφάλειας των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ και των διαδικασιών ΤΠΕ στην Ένωση και να βελτιωθεί η λειτουργία της εσωτερικής αγοράς. Η πρώτη τέτοια αξιολόγηση διενεργείται έως τις 31 Δεκεμβρίου 2023 και οι ακόλουθες αξιολογήσεις διενεργούνται τουλάχιστον ανά διετία εν συνεχεία. Η Επιτροπή, βασιζόμενη στα αποτελέσματα της εν λόγω αξιολόγησης, προσδιορίζει τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ και τις διαδικασίες ΤΠΕ που καλύπτονται από ήδη υφιστάμενο σύστημα πιστοποίησης και τα οποία πρέπει να καλυφθούν από υποχρεωτικό σύστημα πιστοποίησης.

Κατά προτεραιότητα, η Επιτροπή επικεντρώνει την προσοχή της στους τομείς που απαριθμούνται στο παράρτημα ΙΙ της οδηγίας (ΕΕ) 2016/1148 και που αξιολογούνται το αργότερο δύο έτη μετά την έγκριση του πρώτου ευρωπαϊκού συστήματος πιστοποίησης της κυβερνοασφάλειας.

Κατά την εκπόνηση της αξιολόγησης, η Επιτροπή:

α) λαμβάνει υπόψη τον αντίκτυπο των μέτρων στους κατασκευαστές ή τους παρόχους των εν λόγω προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ και στους χρήστες από άποψη κόστους των εν λόγω μέτρων και τα κοινωνικά ή οικονομικά οφέλη που προκύπτουν από το αναμενόμενο βελτιωμένο επίπεδο ασφάλειας για τα στοχευόμενα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ και τις διαδικασίες ΤΠΕ,

β) λαμβάνει υπόψη την ύπαρξη και την εφαρμογή του ισχύοντος δικαίου κράτους μέλους και τρίτης χώρας,

γ) προβαίνει σε ανοικτή, διαφανή και χωρίς αποκλεισμούς διαδικασία διαβούλευσης με όλους τους σχετικούς συμφεροντούχους και τα κράτη μέλη,

δ) λαμβάνει υπόψη τις προθεσμίες εφαρμογής, τα μεταβατικά μέτρα και χρονικά διαστήματα, ιδίως όσον αφορά τις πιθανές συνέπειες του μέτρου για τους κατασκευαστές ή παρόχους προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ, συμπεριλαμβανομένων των ΜΜΕ,

ε) προτείνει τον πλέον ταχύ και αποτελεσματικό τρόπο υλοποίησης της μετάβασης από προαιρετικό σε υποχρεωτικό σύστημα πιστοποίησης.

4. Οι οργανισμοί αξιολόγησης της συμμόρφωσης που αναφέρονται στο άρθρο 60 εκδίδουν ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας δυνάμει του παρόντος άρθρου που αναφέρονται σε «βασικό» ή «σημαντικό» επίπεδο διασφάλισης βάσει κριτηρίων περιλαμβανομένων στο ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας που θεσπίζεται από την Επιτροπή δυνάμει του άρθρου 49.

5. Κατά παρέκκλιση από την παράγραφο 4, σε δεόντως αιτιολογημένες περιπτώσεις ένα ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας μπορεί να προβλέπει ότι τα ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας που προκύπτουν από το εν λόγω σύστημα μπορούν να εκδίδονται μόνο από δημόσιο οργανισμό. Ένας τέτοιος οργανισμός μπορεί να είναι ένα από τα ακόλουθα:

α) μια εθνική αρχή πιστοποίησης της κυβερνοασφάλειας όπως αναφέρεται στο άρθρο 58 παράγραφος 1 ή

β) ένας δημόσιος οργανισμός που λαμβάνει διαπίστευση ως οργανισμός αξιολόγησης της συμμόρφωσης δυνάμει του άρθρου 60 παράγραφος 1.

6. Όταν ένα ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας που εγκρίνεται δυνάμει του άρθρου 49 απαιτεί «υψηλό» επίπεδο διασφάλισης, το ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας δυνάμει του εν λόγω συστήματος μπορεί να εκδοθεί μόνο από εθνική αρχή πιστοποίησης της κυβερνοασφάλειας ή στις ακόλουθες περιπτώσεις, από οργανισμό αξιολόγησης της συμμόρφωσης:

α) κατόπιν προηγούμενης έγκρισης από εθνική αρχή πιστοποίησης της κυβερνοασφάλειας για κάθε ατομικό ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας που εκδίδεται από οργανισμό αξιολόγησης της συμμόρφωσης ή

β) βάσει γενικής ανάθεσης του καθήκοντος έκδοσης των εν λόγω ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας σε οργανισμό αξιολόγησης της συμμόρφωσης από την εθνική αρχή πιστοποίησης της κυβερνοασφάλειας.

7. Το φυσικό ή νομικό πρόσωπο που υποβάλλει τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ ή τις διαδικασίες ΤΠΕ προς πιστοποίηση θέτει στη διάθεση στην εθνική αρχή πιστοποίησης της κυβερνοασφάλειας που αναφέρεται στο άρθρο 58, σε περίπτωση που η εν λόγω αρχή είναι ο οργανισμός που εκδίδει το ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας, ή του οργανισμού αξιολόγησης της συμμόρφωσης που αναφέρεται στο άρθρο 60 όλες τις πληροφορίες που απαιτούνται για τη διενέργεια της πιστοποίησης.

8. Ο κάτοχος ευρωπαϊκού πιστοποιητικού κυβερνοασφάλειας ενημερώνει την αρχή ή τον οργανισμό που αναφέρεται στην παράγραφο 7 για τυχόν τρωτά σημεία ή παρατυπίες που εντοπίστηκαν σε μεταγενέστερο στάδιο σχετικά με την ασφάλεια του πιστοποιημένου προϊόντος ΤΠΕ, υπηρεσίας ΤΠΕ ή διαδικασίας ΤΠΕ και μπορεί να έχουν αντίκτυπο στη συμμόρφωσή του με τις απαιτήσεις σχετικά με την πιστοποίηση. Η εν λόγω αρχή ή οργανισμός διαβιβάζει τις εν λόγω πληροφορίες χωρίς αδικαιολόγητη καθυστέρηση στην ενδιαφερόμενη εθνική αρχή πιστοποίησης της κυβερνοασφάλειας.

9. Ένα ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας εκδίδεται για την περίοδο που προσδιορίζεται στο ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας και μπορεί να ανανεώνεται, με την προϋπόθεση ότι εξακολουθούν να πληρούνται οι σχετικές απαιτήσεις.

10. Ένα ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας που εκδίδεται δυνάμει του παρόντος άρθρου αναγνωρίζεται σε όλα τα κράτη μέλη.

Άρθρο 57

Εθνικά συστήματα πιστοποίησης της κυβερνοασφάλειας και σχετικά πιστοποιητικά

1. Με την επιφύλαξη της παραγράφου 3 του παρόντος άρθρου, τα εθνικά συστήματα πιστοποίησης της κυβερνοασφάλειας και οι σχετικές διαδικασίες για τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ και τις διαδικασίες ΤΠΕ που καλύπτονται από ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας παύουν να παράγουν αποτελέσματα από την ημερομηνία που ορίζεται στην εκτελεστική πράξη που εκδίδεται σύμφωνα με το άρθρο 49 παράγραφος 7. Τα εθνικά συστήματα πιστοποίησης της κυβερνοασφάλειας και οι σχετικές διαδικασίες για τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ και τις διαδικασίες ΤΠΕ που δεν καλύπτονται από ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας εξακολουθούν να παράγουν αποτελέσματα.

2. Τα κράτη μέλη δεν θεσπίζουν νέα εθνικά συστήματα πιστοποίησης της κυβερνοασφάλειας για τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ και τις διαδικασίες ΤΠΕ που καλύπτονται ήδη από ισχύον ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας.

3. Τα υφιστάμενα πιστοποιητικά που έχουν εκδοθεί στο πλαίσιο εθνικών συστημάτων πιστοποίησης της κυβερνοασφάλειας και καλύπτονται από ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας παραμένουν σε ισχύ έως την ημερομηνία λήξης τους.

4. Προκειμένου να αποφευχθεί ο κατακερματισμός της εσωτερικής αγοράς, τα κράτη μέλη ενημερώνουν την Επιτροπή και την ΕΟΠΙΚ σχετικά με οποιαδήποτε πρωτοβουλία για την κατάρτιση νέων εθνικών συστημάτων πιστοποίησης της κυβερνοασφάλειας.

Άρθρο 58

Εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας

1. Κάθε κράτος μέλος ορίζει μία ή περισσότερες εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας στο έδαφός του ή, με τη συμφωνία άλλου κράτους μέλους, ορίζει μία ή περισσότερες εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας που είναι εγκατεστημένες στο εν λόγω 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 εθνικών αρχών πιστοποίησης της κυβερνοασφάλειας. Σε περίπτωση που κράτος μέλος ορίζει περισσότερες από μία αρχές, παρέχει επίσης ενημέρωση στην Επιτροπή σχετικά με τα καθήκοντα που ανατίθενται σε κάθε μία από τις εν λόγω αρχές.

3. Με την επιφύλαξη του άρθρου 56 παράγραφος 5 στοιχείο α) και του άρθρου 56 παράγραφος 6, κάθε εθνική αρχή πιστοποίησης της κυβερνοασφάλειας είναι ανεξάρτητη από τις οντότητες τις οποίες επιβλέπει σε επίπεδο οργάνωσης, αποφάσεων χρηματοδότησης, νομικής διάρθρωσης και λήψης αποφάσεων.

4. Τα κράτη μέλη διασφαλίζουν ότι οι δραστηριότητες των εθνικών αρχών πιστοποίησης της κυβερνοασφάλειας που σχετίζονται με την έκδοση ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας σύμφωνα που αναφέρονται στο άρθρο 56 παράγραφος 5 στοιχείο α) και στο άρθρο 56 παράγραφος 6 είναι αυστηρά διαχωρισμένες από τις εποπτικές δραστηριότητές τους που καθορίζονται στο παρόν άρθρο και ότι οι εν λόγω δραστηριότητες διενεργούνται ανεξάρτητα μεταξύ τους.

5. Τα κράτη μέλη μεριμνούν ώστε οι εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας να έχουν στη διάθεσή τους επαρκείς πόρους για την άσκηση των αρμοδιοτήτων τους και να ασκούν, με αποδοτικό και αποτελεσματικό τρόπο, τα καθήκοντά τους.

6. Για την αποτελεσματική εφαρμογή του παρόντος κανονισμού, οι εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας είναι σκόπιμο να συμμετέχουν στην ΕΟΠΙΚ με ενεργό, αποτελεσματικό, αποδοτικό και ασφαλή τρόπο.

7. Οι εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας:

α) εποπτεύουν και μεριμνούν για την εφαρμογή των κανόνων που περιλαμβάνονται στα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας σύμφωνα με το άρθρο 54 παράγραφος 1 στοιχείο ι) για την παρακολούθηση της συμμόρφωσης των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ και των διαδικασιών ΤΠΕ προς τις απαιτήσεις των ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας που έχουν εκδοθεί στα αντίστοιχα εδάφη τους, σε συνεργασία με άλλες αρμόδιες αρχές εποπτείας της αγοράς,

β) παρακολουθούν τη συμμόρφωση με τις υποχρεώσεις των κατασκευαστών ή των παρόχων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ που είναι εγκατεστημένοι στα αντίστοιχα εδάφη τους και που διενεργούν αυτοαξιολόγηση συμμόρφωσης και επιβάλλουν την εφαρμογή των εν λόγω υποχρεώσεων και παρακολουθούν ιδίως τη συμμόρφωση με τις υποχρεώσεις των εν λόγω κατασκευαστών ή παρόχων που προβλέπονται στο άρθρο 53 παράγραφοι 2 και 3 και στο αντίστοιχο ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας και επιβάλλουν την εφαρμογή των εν λόγω υποχρεώσεων,

γ) με την επιφύλαξη του άρθρου 60 παράγραφος 3, παρέχουν ενεργό βοήθεια και υποστήριξη στους εθνικούς οργανισμούς διαπίστευσης για την παρακολούθηση και την εποπτεία των δραστηριοτήτων των οργανισμών αξιολόγησης της συμμόρφωσης για τους σκοπούς του παρόντος κανονισμού,

δ) παρακολουθούν και εποπτεύουν τις δραστηριότητες των δημόσιων οργανισμών που αναφέρονται στο άρθρο 56 παράγραφος 5,

ε) κατά περίπτωση, εξουσιοδοτούν τους οργανισμούς αξιολόγησης της συμμόρφωσης σύμφωνα με το άρθρο 60 παράγραφος 3 και περιορίζουν, αναστέλλουν ή ανακαλούν υπάρχουσα αδειοδότηση όταν οι οργανισμοί αξιολόγησης της συμμόρφωσης παραβαίνουν τις απαιτήσεις του παρόντος κανονισμού,

στ) διεκπεραιώνουν καταγγελίες από φυσικά ή νομικά πρόσωπα σε σχέση με ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας που έχουν εκδοθεί από εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας ή σε σχέση με ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας που έχουν εκδοθεί από οργανισμούς αξιολόγησης της συμμόρφωσης σύμφωνα με το άρθρο 56 παράγραφος 6 ή σε σχέση με τις δηλώσεις συμμόρφωσης ΕΕ που εκδίδονται δυνάμει του άρθρου 53, και διερευνούν το αντικείμενο των εν λόγω καταγγελιών στον βαθμό που ενδείκνυται και ενημερώνουν τον καταγγέλλοντα σχετικά με την πρόοδο και το αποτέλεσμα της έρευνας εντός εύλογου χρονικού διαστήματος,

ζ) εκπονούν ετήσια συνοπτική έκθεση σχετικά με τις δραστηριότητες που διενεργούν, σύμφωνα με τα στοιχεία β), γ) και δ) της παρούσας παραγράφου ή την παράγραφο 8, με αποδέκτη τον ENISA και την ΕΟΠΙΚ,

η) συνεργάζονται με άλλες εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας ή άλλες δημόσιες αρχές, μεταξύ άλλων μέσω της ανταλλαγής πληροφοριών σχετικά με πιθανή μη συμμόρφωση προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ με τις απαιτήσεις του παρόντος κανονισμού ή με τις απαιτήσεις συγκεκριμένων ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας, και

θ) παρακολουθούν τις σχετικές εξελίξεις στον τομέα της πιστοποίησης της κυβερνοασφάλειας.

8. Κάθε εθνική αρχή πιστοποίησης της κυβερνοασφάλειας έχει κατ' ελάχιστον τις ακόλουθες εξουσίες:

α) να ζητά από τους οργανισμούς αξιολόγησης της συμμόρφωσης, τους κατόχους ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας και τους εκδότες δηλώσεων συμμόρφωσης ΕΕ να προσκομίσουν τις πληροφορίες που απαιτούνται για την άσκηση των καθηκόντων τους,

β) να διενεργεί έρευνες, υπό μορφή ελέγχων, των οργανισμών αξιολόγησης της συμμόρφωσης, των κατόχων ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας και των εκδοτών δηλώσεων συμμόρφωσης ΕΕ, με στόχο τον έλεγχο της συμμόρφωσής τους με τις διατάξεις του παρόντος τίτλου,

γ) να λαμβάνει τα ενδεδειγμένα μέτρα, σύμφωνα με το εθνικό δίκαιο, προκειμένου να διασφαλίζεται η συμμόρφωση των οργανισμών αξιολόγησης της συμμόρφωσης, των κατόχων ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας και των εκδοτών δηλώσεων συμμόρφωσης ΕΕ με τον παρόντα κανονισμό ή με ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας,

δ) να έχει πρόσβαση στους χώρους οποιωνδήποτε οργανισμών αξιολόγησης της συμμόρφωσης ή των κατόχων ευρωπαϊκών πιστοποιητικών της κυβερνοασφάλειας, με σκοπό τη διενέργεια ερευνών σύμφωνα με το δικονομικό δίκαιο της Ένωσης ή των κρατών μελών,

ε) να ανακαλεί, σύμφωνα με το εθνικό δίκαιο, ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας που έχουν εκδοθεί από εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας ή ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας που έχουν εκδοθεί από οργανισμούς αξιολόγησης της συμμόρφωσης, σύμφωνα με το άρθρο 56 παράγραφος 6, όταν τα εν λόγω πιστοποιητικά δεν συμμορφώνονται με τον παρόντα κανονισμό ή με ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας,

στ) να επιβάλλει κυρώσεις σε συμφωνία με το εθνικό δίκαιο, όπως προβλέπεται στο άρθρο 65, και να απαιτεί άμεση παύση των παραβιάσεων των υποχρεώσεων οι οποίες θεσπίζονται στον παρόντα κανονισμό.

9. Οι εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας συνεργάζονται μεταξύ τους και με την Επιτροπή, ιδίως ανταλλάσσοντας πληροφορίες, εμπειρίες και ορθές πρακτικές όσον αφορά την πιστοποίηση της κυβερνοασφάλειας και τα τεχνικά ζητήματα που αφορούν την κυβερνοασφάλεια των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ και των διαδικασιών ΤΠΕ.

Άρθρο 59

Αξιολόγηση από ομοτίμους

1. Με σκοπό την επίτευξη ισοδύναμων προτύπων σε ολόκληρη την Ένωση όσον αφορά τα ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας και τις δηλώσεις συμμόρφωσης ΕΕ, οι εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας υπόκεινται σε αξιολόγηση από ομοτίμους.

2. Η αξιολόγηση από ομοτίμους πραγματοποιείται με βάση αυστηρά και διαφανή κριτήρια και διαδικασίες αξιολόγησης, ιδιαίτερα όσον αφορά τις απαιτήσεις σε επίπεδο διάρθρωσης, ανθρώπινων πόρων και διεργασίας, την εμπιστευτικότητα και τις καταγγελίες.

3. Η αξιολόγηση από ομοτίμους καλύπτει:

α) κατά περίπτωση, αν οι δραστηριότητες των εθνικών αρχών πιστοποίησης της κυβερνοασφάλειας που σχετίζονται με την έκδοση ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας που αναφέρονται στο άρθρο 56 παράγραφος 5 στοιχείο α) και στο άρθρο 56 παράγραφος 6 είναι αυστηρά διαχωρισμένες από τις εποπτικές δραστηριότητές τους που καθορίζονται στο άρθρο 58 και αν οι εν λόγω δραστηριότητες διενεργούνται ανεξάρτητα μεταξύ τους,

β) τις διαδικασίες για την εποπτεία και την επιβολή των κανόνων παρακολούθησης της συμμόρφωσης των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ και των διαδικασιών ΤΠΕ με ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας δυνάμει του άρθρου 58 παράγραφος 7 στοιχείο α),

γ) τις διαδικασίες για την παρακολούθηση και την τήρηση των υποχρεώσεων των κατασκευαστών ή των παρόχων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ δυνάμει του άρθρου 58 παράγραφος 7 στοιχείο β),

δ) τις διαδικασίες για την παρακολούθηση, την έγκριση και την εποπτεία των δραστηριοτήτων των οργανισμών αξιολόγησης της συμμόρφωσης,

ε) κατά περίπτωση, αν το προσωπικό των αρχών ή των οργανισμών που εκδίδουν πιστοποιητικά για «υψηλό» επίπεδο διασφάλισης δυνάμει του άρθρου 56 παράγραφος 6 διαθέτει την κατάλληλη εμπειρογνωσία.

4. Αξιολόγηση από ομοτίμους διενεργείται από τουλάχιστον δύο εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας που ανήκουν σε άλλα κράτη μέλη και από την Επιτροπή με συχνότητα τουλάχιστον μία φορά ανά πέντε έτη. Ο ENISA δύναται να συμμετέχει στην αξιολόγηση από ομοτίμους.

5. Η Επιτροπή μπορεί να εκδίδει εκτελεστικές πράξεις για την κατάρτιση σχεδίου αξιολογήσεων από ομοτίμους που να καλύπτει περίοδο τουλάχιστον πέντε ετών, να ορίζει τα κριτήρια για τη σύνθεση της ομάδας αξιολόγησης από ομοτίμους, τη μεθοδολογία που πρέπει να χρησιμοποιείται για την αξιολόγηση από ομοτίμους και το χρονοδιάγραμμα, τη συχνότητα και τα λοιπά καθήκοντα που σχετίζονται με αυτήν. Κατά την έγκριση των εν λόγω εκτελεστικών πράξεων, η Επιτροπή λαμβάνει δεόντως υπόψη τις απόψεις της ΕΟΠΙΚ. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 66 παράγραφος 2.

6. Τα αποτελέσματα των αξιολογήσεων από ομοτίμους εξετάζονται από την ΕΟΠΙΚ, η οποία εκπονεί συνοπτικές εκθέσεις που μπορούν να καταστούν διαθέσιμες στο κοινό και, εφόσον απαιτείται, εκδίδει κατευθυντήριες γραμμές ή συστάσεις για δράσεις ή μέτρα που πρέπει να λάβουν οι ενδιαφερόμενοι φορείς.

Άρθρο 60

Οργανισμοί αξιολόγησης της συμμόρφωσης

1. Οι οργανισμοί αξιολόγησης της συμμόρφωσης λαμβάνουν διαπίστευση από εθνικούς οργανισμούς διαπίστευσης που ορίζονται σύμφωνα με τον κανονισμό (ΕΚ) αριθ. 765/2008. Η εν λόγω διαπίστευση λαμβάνεται μόνο εφόσον ο οργανισμός αξιολόγησης της συμμόρφωσης πληροί τις απαιτήσεις που θεσπίζονται στο παράρτημα του παρόντος κανονισμού.

2. Όταν εκδίδεται ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας από εθνική αρχή πιστοποίησης της κυβερνοασφάλειας δυνάμει του άρθρου 56 παράγραφος 5 στοιχείο α) και του άρθρου 56 παράγραφος 6, ο οργανισμός πιστοποίησης της εθνικής αρχής πιστοποίησης της κυβερνοασφάλειας λαμβάνει διαπίστευση ως οργανισμός αξιολόγησης της συμμόρφωσης δυνάμει της παραγράφου 1 του παρόντος άρθρου.

3. Σε περιπτώσεις που ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας ορίζουν ειδικές ή επιπρόσθετες απαιτήσεις δυνάμει του άρθρου 54 παράγραφος 1 στοιχείο στ), μόνο οργανισμοί αξιολόγησης της συμμόρφωσης που πληρούν τις εν λόγω απαιτήσεις εγκρίνονται από την εθνική αρχή πιστοποίησης της κυβερνοασφάλειας για να εκτελούν καθήκοντα στο πλαίσιο των εν λόγω συστημάτων.

4. Η διαπίστευση που αναφέρεται στην παράγραφο 1 χορηγείται στους οργανισμούς αξιολόγησης της συμμόρφωσης για μέγιστο χρονικό διάστημα πέντε ετών και μπορεί να ανανεωθεί με τους ίδιους όρους, υπό την προϋπόθεση ότι ο οργανισμός αξιολόγησης της συμμόρφωσης εξακολουθεί να πληροί τις απαιτήσεις του παρόντος άρθρου. Οι εθνικοί 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 που χορηγήθηκε βάσει της παραγράφου 1 όταν δεν πληρούνται ή δεν πληρούνται πλέον οι όροι για τη διαπίστευση ή όταν ο οργανισμός αξιολόγησης της συμμόρφωσης παραβιάζουν τον παρόντα κανονισμό.

Άρθρο 61

Κοινοποίηση

1. Για κάθε ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας, οι εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας κοινοποιούν στην Επιτροπή τους οργανισμούς αξιολόγησης της συμμόρφωσης που είναι διαπιστευμένοι και, κατά περίπτωση, εξουσιοδοτημένοι δυνάμει του άρθρου 60 παράγραφος 3 να εκδίδουν ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας σε συγκεκριμένα επίπεδα διασφάλισης όπως αναφέρεται στο άρθρο 52. Η εθνική αρχή πιστοποίησης της κυβερνοασφάλειας κοινοποιεί στην Επιτροπή κάθε μεταγενέστερη σχετική μεταβολή, χωρίς αδικαιολόγητη καθυστέρηση.

2. Με τη συμπλήρωση έτους από την έναρξη εφαρμογής ενός ευρωπαϊκού συστήματος πιστοποίησης της κυβερνοασφάλειας, η Επιτροπή δημοσιεύει κατάλογο των κοινοποιηθέντων δυνάμει του εν λόγω συστήματος οργανισμών αξιολόγησης της συμμόρφωσης στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

3. Εάν η Επιτροπή λάβει κοινοποίηση μετά την πάροδο του αναφερόμενου στην παράγραφο 2 χρονικού διαστήματος, δημοσιεύει στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης* τις τροποποιήσεις του καταλόγου των οργανισμών αξιολόγησης της συμμόρφωσης εντός δύο μηνών από την ημερομηνία παραλαβής της εν λόγω κοινοποίησης.

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

5. Η Επιτροπή δύναται να εκδίδει εκτελεστικές πράξεις για τον καθορισμό των συνθηκών, της μορφής και των διαδικασιών 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 66 παράγραφος 2.

Άρθρο 62

Ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας

1. Συστήνεται ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας («ΕΟΠΙΚ»).

2. Η ΕΟΠΙΚ απαρτίζεται από αντιπροσώπους των εθνικών αρχών πιστοποίησης της κυβερνοασφάλειας ή αντιπροσώπους άλλων σχετικών εθνικών αρχών. Ένα μέλος της ΕΟΠΙΚ δεν αντιπροσωπεύει περισσότερα από δύο κράτη μέλη.

3. Οι συμφεροντούχοι και οι σχετικοί τρίτοι μπορούν να καλούνται να παρίστανται στις συνεδριάσεις της ΕΟΠΙΚ και να συμμετέχουν στις εργασίες της.

4. Η ΕΟΠΙΚ έχει τα ακόλουθα καθήκοντα:

α) να συμβουλεύει και να επικουρεί την Επιτροπή στην προσπάθειά της να διασφαλίσει τη συνεπή υλοποίηση και εφαρμογή του παρόντος τίτλου, ιδίως όσον αφορά το κυλιόμενο πρόγραμμα εργασίας της Ένωσης, τα ζητήματα της πολιτικής πιστοποίησης της κυβερνοασφάλειας, τον συντονισμό των προσεγγίσεων πολιτικής, και την επεξεργασία ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας,

β) να επικουρεί, να συμβουλεύει και να συνεργάζεται με τον ENISA κατά την επεξεργασία ενός υποψήφιου συστήματος δυνάμει του άρθρου 49,

γ) να εκδίδει γνώμη σχετικά με υποψήφια συστήματα που επεξεργάζεται ο ENISA δυνάμει του άρθρου 49,

δ) να υποβάλλει αίτημα στον ENISA προκειμένου να προχωρήσει στην επεξεργασία υποψήφιου συστήματος δυνάμει του άρθρου 48 παράγραφος 2,

ε) να εκδίδει γνώμες που απευθύνονται στην Επιτροπή σχετικά με τη διατήρηση και επανεξέταση των υφιστάμενων ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας,

στ) να εξετάζει τις σχετικές εξελίξεις στον τομέα της πιστοποίησης της κυβερνοασφάλειας και να ανταλλάσσει πληροφορίες και ορθές πρακτικές σε σχέση με τα συστήματα πιστοποίησης της κυβερνοασφάλειας,

ζ) να διευκολύνει τη συνεργασία μεταξύ των εθνικών αρχών πιστοποίησης της κυβερνοασφάλειας βάσει του παρόντος τίτλου μέσω της ανάπτυξης ικανοτήτων και της ανταλλαγής πληροφοριών, καθιερώνοντας, ειδικότερα, μεθόδους για την αποτελεσματική ανταλλαγή πληροφοριών σχετικά με θέματα που αφορούν την πιστοποίηση της κυβερνοασφάλειας,

η) να υποστηρίζει την εφαρμογή του μηχανισμού αξιολόγησης από ομοτίμους σύμφωνα με τους κανόνες που καθορίζονται σε ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας δυνάμει του άρθρου 54 παράγραφος 1 στοιχείο κα),

θ) να διευκολύνει την ευθυγράμμιση των υφιστάμενων ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας με τα διεθνώς αναγνωρισμένα σχετικά πρότυπα, μεταξύ άλλων επανεξετάζοντας τα υφιστάμενα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας, και, κατά περίπτωση, προβαίνοντας στη διατύπωση συστάσεων προς τον ENISA για τη συνεργασία με σχετικούς διεθνείς οργανισμούς πιστοποίησης για την αντιμετώπιση ανεπαρκειών ή κενών σε διαθέσιμα διεθνώς αναγνωρισμένα πρότυπα.

5. Με τη συνδρομή του ENISA, η Επιτροπή προεδρεύει της ΕΟΠΙΚ και της παρέχει γραμματειακή υποστήριξη σύμφωνα με το άρθρο 8 παράγραφος 1 στοιχείο ε).

Άρθρο 63

Δικαίωμα υποβολής καταγγελίας

1. Τα φυσικά και τα νομικά πρόσωπα έχουν το δικαίωμα να υποβάλλουν καταγγελία προς τον εκδότη ευρωπαϊκού πιστοποιητικού κυβερνοασφάλειας ή, όταν η καταγγελία αφορά ευρωπαϊκό πιστοποιητικό κυβερνοασφάλειας εκδιδόμενο από οργανισμό αξιολόγησης της συμμόρφωσης ενεργούντα σύμφωνα με το άρθρο 56 παράγραφος 6, προς την αρμόδια εθνική αρχή πιστοποίησης της κυβερνοασφάλειας.

2. Η αρχή ή ο οργανισμός στον οποίο έχει υποβληθεί η καταγγελία ενημερώνει τον καταγγέλλοντα για την πρόοδο της διαδικασίας και για τη ληφθείσα απόφαση και ενημερώνει τον καταγγέλλοντα για το δικαίωμα άσκησης πραγματικής δικαστικής προσφυγής όπως αναφέρεται στο άρθρο 64.

Άρθρο 64

Δικαίωμα πραγματικής δικαστικής προσφυγής

1. Παρά τη δυνατότητα διοικητικών ή άλλων εξωδικαστικών λύσεων, τα φυσικά και τα νομικά πρόσωπα έχουν το δικαίωμα να ασκήσουν πραγματική δικαστική προσφυγή με αντικείμενο:

α) αποφάσεις που λαμβάνονται από την αρχή ή τον οργανισμό που αναφέρεται στο άρθρο 63 παράγραφος 1, μεταξύ άλλων όσον αφορά, κατά περίπτωση, την αντικανονική έκδοση, την παράλειψη έκδοσης ή την αναγνώριση ευρωπαϊκού πιστοποιητικού κυβερνοασφάλειας το οποίο έχουν στην κατοχή τους τα εν λόγω φυσικά και νομικά πρόσωπα,

β) παράλειψη να δοθεί συνέχεια σε καταγγελία που έχει υποβληθεί σε αρχή ή οργανισμό που αναφέρεται στο άρθρο 63 παράγραφος 1.

2. Οι διαδικασίες που προβλέπονται στο παρόν άρθρο εκδικάζονται από τα δικαστήρια του κράτους μέλους όπου είναι εγκατεστημένη η αρχή ή ο οργανισμός κατά του οποίου ασκείται η δικαστική προσφυγή.

Άρθρο 65

Κυρώσεις

Τα κράτη μέλη καθορίζουν τους κανόνες για τις κυρώσεις οι οποίες επιβάλλονται σε περίπτωση παραβίασης του παρόντος τίτλου και παραβίασης των ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας 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 χωρίς καθυστέρηση τους εν λόγω κανόνες και μέτρα και την ενημερώνουν σχετικά με κάθε μεταγενέστερη τροποποίησή τους.

ΤΙΤΛΟΣ IV

ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 66

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 67

Αξιολόγηση και επανεξέταση

1. Έως τις 28 Ιουνίου 2024 και στη συνέχεια ανά πενταετία, η Επιτροπή αξιολογεί τον αντίκτυπο, την αποτελεσματικότητα και την απόδοση του ENISA και των εργασιακών πρακτικών του, τη δυνατότητα για ενδεχόμενη τροποποίηση της εντολής του ENISA, και τις δημοσιονομικές επιπτώσεις οποιασδήποτε τέτοιας τροποποίησης. Στην αξιολόγηση λαμβάνονται υπόψη οι αντιδράσεις που έχουν παρασχεθεί στον ENISA σε σχέση με τις δραστηριότητές του. Σε περίπτωση που η Επιτροπή κρίνει ότι οι στόχοι, η εντολή και τα καθήκοντά που του έχουν ανατεθεί δεν δικαιολογούν πλέον τη συνέχιση της λειτουργίας του ENISA, η Επιτροπή μπορεί να εισηγηθεί την τροποποίηση του παρόντος κανονισμού ως προς τις διατάξεις που αφορούν τον ENISA.

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

3. Η αξιολόγηση εκτιμά κατά πόσον είναι απαραίτητες βασικές απαιτήσεις κυβερνοασφάλειας για την πρόσβαση στην εσωτερική αγορά, ώστε να αποφευχθεί η είσοδος προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ που δεν πληρούν τις βασικές απαιτήσεις κυβερνοασφάλειας στην αγορά της Ένωσης.

4. Έως τις 28 Ιουνίου 2024 και στη συνέχεια ανά πενταετία, η Επιτροπή διαβιβάζει την έκθεση αξιολόγησης μαζί με τα συμπεράσματά της στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και το διοικητικό συμβούλιο. Τα συμπεράσματα της εν λόγω έκθεσης δημοσιοποιούνται.

Άρθρο 68

Κατάργηση και διαδοχή

1. Ο κανονισμός (ΕΕ) αριθ. 526/2013 καταργείται από τις 27 Ιουνίου 2019.

2. Οι παραπομπές στον κανονισμό (ΕΕ) αριθ. 526/2013 και στον ENISA όπως συστάθηκε με τον εν λόγω κανονισμό θεωρείται ότι αποτελούν παραπομπές στον παρόντα κανονισμό και στον ENISA όπως συστήνεται με τον παρόντα κανονισμό.

3. Ο ENISA όπως συστήνεται με τον παρόντα κανονισμό διαδέχεται τον ENISA όπως συστάθηκε με τον κανονισμό (ΕΕ) αριθ. 526/2013 όσον αφορά όλα τα δικαιώματα ιδιοκτησίας, τις συμφωνίες, τις νομικές υποχρεώσεις, τις συμβάσεις εργασίας, τις οικονομικές δεσμεύσεις και ευθύνες. Όλες οι αποφάσεις του διοικητικού συμβουλίου και του εκτελεστικού συμβουλίου που εκδόθηκαν σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 526/2013 παραμένουν σε ισχύ, εφόσον συμμορφώνονται με τον παρόντα κανονισμό.

4. Ο ENISA ιδρύεται για απεριόριστο χρονικό διάστημα από τις 27 Ιουνίου 2019.

5. Ο εκτελεστικός διευθυντής που διορίζεται βάσει του άρθρου 24 παράγραφος 4 του κανονισμού (ΕΕ) αριθ. 526/2013 παραμένει σε υπηρεσία και ασκεί τα καθήκοντα του εκτελεστικού διευθυντή όπως αναφέρονται στο άρθρο 20 του παρόντος κανονισμού για το υπόλοιπο της θητείας του. Οι λοιποί όροι της σύμβασής του παραμένουν αμετάβλητοι.

6. Τα τακτικά μέλη του διοικητικού συμβουλίου και τα αναπληρωματικά μέλη τους που διορίζονται βάσει του άρθρου 6 του κανονισμού (ΕΕ) αριθ. 526/2013 παραμένουν σε υπηρεσία και ασκούν τα καθήκοντα του διοικητικού συμβουλίου όπως αναφέρονται στο άρθρο 15 του παρόντος κανονισμού για το υπόλοιπο της θητείας τους.

Άρθρο 69

Έναρξη ισχύος

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

2. Τα άρθρα 58, 60, 61, 63, 64 και 65 εφαρμόζονται από τις 28 Ιουνίου 2021.

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

Στρασβούργο, 17 Απριλίου 2019.

Για το Ευρωπαϊκό Κοινοβούλιο	*Για το Συμβούλιο*
Ο Πρόεδρος	*Ο Πρόεδρος*
A. TAJANI	G. CIAMBA

ΠΑΡΑΡΤΗΜΑ

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 του εθνικού δικαίου και διαθέτει νομική προσωπικότητα.

2. Ο οργανισμός αξιολόγησης της συμμόρφωσης είναι τρίτος φορέας, ανεξάρτητος από τον οργανισμό ή τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ ή τις διαδικασίες 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 ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών 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 τα πρόσωπα που είναι αρμόδια 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 ΤΠΕ, της υπηρεσίας ΤΠΕ ή της διαδικασίας ΤΠΕ που αξιολογείται, ούτε ο εξουσιοδοτημένος αντιπρόσωπος των ανωτέρω. Η εν λόγω απαγόρευση δεν αποκλείει τη χρήση των αξιολογημένων προϊόντων ΤΠΕ που είναι αναγκαία για τις λειτουργίες του οργανισμού αξιολόγησης της συμμόρφωσης ή τη χρήση των εν λόγω προϊόντων ΤΠΕ για προσωπικούς σκοπούς.

5. Οι οργανισμοί αξιολόγησης της συμμόρφωσης, τα διευθυντικά του στελέχη και τα πρόσωπα που είναι αρμόδια 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 προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ ή των διαδικασιών ΤΠΕ που αξιολογούνται, ούτε εκπροσωπούν μέρη που εμπλέκονται στις εν λόγω δραστηριότητες. Οι οργανισμοί αξιολόγησης της συμμόρφωσης, τα διευθυντικά του στελέχη και τα πρόσωπα που είναι αρμόδια για την εκτέλεση των καθηκόντων αξιολόγησης της συμμόρφωσης δεν αναλαμβάνουν καμιά δραστηριότητα που μπορεί να έλθει σε σύγκρουση με την ανεξάρτητη κρίση ή την ακεραιότητά τους σε σχέση με τις οικείες δραστηριότητες αξιολόγησης της συμμόρφωσης. Η εν λόγω απαγόρευση ισχύει ιδίως για συμβουλευτικές υπηρεσίες.

6. Εάν ένας οργανισμός αξιολόγησης της συμμόρφωσης ανήκει ή ελέγχεται από δημόσιο οργανισμό ή φορέα, διασφαλίζεται και τεκμηριώνεται η ανεξαρτησία και η απουσία οποιασδήποτε σύγκρουσης συμφερόντων μεταξύ της εθνικής αρχής πιστοποίησης της κυβερνοασφάλειας και του οργανισμού αξιολόγησης της συμμόρφωσης.

7. 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.

8. Οι οργανισμοί αξιολόγησης της συμμόρφωσης και το προσωπικό τους εκτελούν 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 που θα ήταν δυνατόν να επηρεάσει την κρίση τους ή τα αποτελέσματα των οικείων δραστηριοτήτων αξιολόγησης της συμμόρφωσης, συμπεριλαμβανομένων των πιέσεων και προτροπών οικονομικής φύσης, ιδιαίτερα από πρόσωπα ή ομάδες προσώπων που έχουν συμφέρον από τα αποτελέσματα αυτών των δραστηριοτήτων.

9. 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, ανεξάρτητα από το αν πρόκειται για καθήκοντα που εκτελούνται από τον ίδιο τον οργανισμό αξιολόγησης της συμμόρφωσης ή εξ ονόματός του και υπό την ευθύνη του. Οποιαδήποτε υπεργολαβική ανάθεση σε εξωτερικό προσωπικό ή διαβούλευση με αυτό τεκμηριώνεται κατάλληλα, δεν περιλαμβάνει κανένα διαμεσολαβητή και διέπεται από γραπτή συμφωνία η οποία καλύπτει, μεταξύ άλλων, τα ζητήματα της εμπιστευτικότητας και της σύγκρουσης συμφερόντων. Ο εν λόγω οργανισμός αξιολόγησης της συμμόρφωσης αναλαμβάνει την πλήρη ευθύνη για τα καθήκοντα που εκτελεί.

10. Ανά πάσα στιγμή και για κάθε διαδικασία αξιολόγησης της συμμόρφωσης και κάθε τύπος, κατηγορία ή υποκατηγορία προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών 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 οφείλεται να διενεργείται αξιολόγηση της συμμόρφωσης, για να διασφαλιστεί η διαφάνεια των εν λόγω διαδικασιών και η δυνατότητα αναπαραγωγής τους. Διαθέτει κατάλληλες πολιτικές και διαδικασίες που διακρίνουν μεταξύ καθηκόντων τα οποία εκτελεί ως δυνάμει του άρθρου 61 κοινοποιημένος οργανισμός και των άλλων δραστηριοτήτων του,

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 ΤΠΕ, της υπηρεσίας ΤΠΕ ή της διαδικασίας ΤΠΕ και τον μαζικό ή εν σειρά χαρακτήρα της παραγωγικής διαδικασίας.

11. 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.

12. Τα πρόσωπα που είναι αρμόδια για τη διεξαγωγή των δραστηριοτήτων αξιολόγησης της συμμόρφωσης διαθέτουν τα ακόλουθα:

α) εις βάθος τεχνική και επαγγελματική κατάρτιση που καλύπτει όλες τις δραστηριότητες αξιολόγησης της συμμόρφωσης,

β) επαρκή γνώση των απαιτήσεων των αξιολογήσεων συμμόρφωσης που διενεργούν 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 καταρτίζουν πιστοποιητικά, πρακτικά και εκθέσεις που αποδεικνύουν τη διεξαγωγή των αξιολογήσεων συμμόρφωσης.

13. Διασφαλίζεται η αμεροληψία των οργανισμών αξιολόγησης της συμμόρφωσης, των διευθυντικών στελεχών τους και των προσώπων που είναι υπεύθυνα για τη διενέργεια δραστηριοτήτων αξιολόγησης συμμόρφωσης και οποιωνδήποτε υπεργολάβων αξιολόγησης.

14. Η αμοιβή των διευθυντικών στελεχών και των προσώπων που είναι υπεύθυνα για τη διενέργεια δραστηριοτήτων αξιολόγησης συμμόρφωσης δεν εξαρτάται από τον αριθμό των διεξαγόμενων αξιολογήσεων συμμόρφωσης ή από τα αποτελέσματα των εν λόγω αξιολογήσεων.

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

16. Ο οργανισμός αξιολόγησης της συμμόρφωσης και το προσωπικό του, οι επιτροπές του, οι θυγατρικές του, οι υπεργολάβοι του και κάθε συνεργαζόμενος φορέας ή το προσωπικό εξωτερικών οργανισμών ενός οργανισμού αξιολόγησης της συμμόρφωσης τηρούν την εμπιστευτικότητα και το επαγγελματικό απόρρητο για κάθε πληροφορία που περιέρχεται εις γνώσιν τους κατά την εκτέλεση των οικείων καθηκόντων αξιολόγησης συμμόρφωσης σύμφωνα με τον παρόντα κανονισμό ή οποιανδήποτε εκτελεστική του παρόντος κανονισμού διάταξη του εθνικού δικαίου, εκτός από την περίπτωση κατά την οποία απαιτείται γνωστοποίηση δυνάμει του ενωσιακού ή εθνικού δικαίου στην οποία υπόκεινται τα εν λόγω πρόσωπα και εκτός εάν πρόκειται για τις αρμόδιες αρχές του κράτους μέλους στο οποίο διεξάγονται οι δραστηριότητές του. Τα δικαιώματα διανοητικής ιδιοκτησίας προστατεύονται. Ο οργανισμός αξιολόγησης της συμμόρφωσης διαθέτει τεκμηριωμένες διαδικασίες σχετικά με τις απαιτήσεις του παρόντος σημείου.

17. Με εξαίρεση το σημείο 16, οι απαιτήσεις του παρόντος παραρτήματος δεν αποκλείουν ανταλλαγές τεχνικών πληροφοριών και ρυθμιστικής καθοδήγησης μεταξύ οργανισμού αξιολόγησης της συμμόρφωσης και προσώπου που υποβάλλει αίτηση πιστοποίησης ή που εξετάζει το ενδεχόμενο να υποβάλει αίτηση πιστοποίησης.

18. Οι οργανισμοί αξιολόγησης της συμμόρφωσης λειτουργούν σύμφωνα με σειρά συνεπών, δίκαιων και εύλογων όρων και προϋποθέσεων, λαμβάνοντας υπόψη τα συμφέροντα των ΜΜΕ σε σχέση με τις αμοιβές.

19. 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 προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ.

20. 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.